数论中的问题与结果

曹珍富　编著

哈尔滨工业大学出版社

内容简介

本书几乎囊括了数论中的全部历史与现代问题，同时对这些问题研究的结果与发表论文的出处作了详细介绍。

全书共六章，分别为：素数、整除、堆垒数论、丢番图方程、整数序列以及一些其它问题。本书是在编译理查德 K. 盖依(Richard K. Guy)所著《数论中尚未解决的问题》(Unsolved Problems in Number Theory)的基础上增加新的问题与结果，同时作适当删减而写成的。其中完全新写的内容有 A18、D2、D5、D9、D25、D26、D27、D28、E28、F20、F30 等。

本书可作为数学工作者、研究生、大学生以及数学爱好者阅读与参考。

数论中的问题与结果
Shulunzhong de Wenti yu Jiegou
曹珍富　编著
*
哈尔滨工业大学出版社出版
新华书店首都发行所发行
哈尔滨市工大节能印刷厂印刷
*
开本 850×1168　1/32　印张 8　字数 230 千字
1996 年 6 月第 1 版　1998 年 4 月第 2 次印刷
印数　1 501—2 500
ISBN 7-5603-1152-0/O・76　定价 12.00 元

前　言

数论是一门古老的数学分支。由于它的问题简明易懂，因此它比任何一个其它数学分支都更吸引人们的注意。许多业余数学爱好者都是从这里起步，通过对数论中的一些问题的探讨，获得了从事数学研究的信心。这一点对初做研究的人来说是非常重要的。

在许多数论问题的研究中我国都处于领先地位，而且自古以来，我们的祖先就已从事数论中某些问题的研究，取得了举世瞩目的成果。象闻名于世的孙子定理(又称中国剩余定理)，它不仅是初等数论中的一个精美定理，而且在计算机科学、通信理论等现代科学技术领域中也得到了相当广泛的应用。早在商高年代，我们的祖先就知道“勾三股四而弦五”的结论，即给出了方程 $x^2+y^2=z^2$ 的一组正整数解 $x=3, y=4, z=5$。这要比古希腊三世纪的丢番图(Diophantus)研究这类方程早多了。在我国现代的数学家中，华罗庚、柯召、闵嗣鹤等老一辈数论学家曾取得过辉煌成就。其中尤以华罗庚教授在解析数论上的工作，是举世公认的。60 年代以来，我国数论学家陈景润、王元、潘承洞等，在筛法与哥德巴赫(Goldbach)猜想等问题上取得了国际上领先的结果。受到他们的鼓舞，我国年轻的数论工作者在许多问题上也取得一系列的新进展。为了使更多的人了解数论中的问题与结果，我在 1987 年 10 月编译了理查德 K. 盖依(Richard K. Guy)著《数论中尚未解决的问题》(Unsolved Problems in Number Theory, Springer-Verlag, New York, 1981)，但由于种种原因没有出版。鉴于盖依教授的书写得非常好，我认为值得向国内广大数学工作者与数学爱好者推荐。现

在，许多问题有了新的进展，而且又有许多新问题被提出来，所以丰富与发展盖依教授的书就是件很有意义的事。本书就是在当时编译书稿的基础上改写的，在保留了原书参考文献的基础上，又增加了许多新文献，并且在原书的框架下，几乎对每个问题均进行了重写，删掉了个别含糢不清的问题，同时增加了若干新的问题与结果，其中有些章节是完全新增的，比如A18，D2，D5，D9，D25，D26，D27，D28，E28，F20，F30等等。

全书共分六章，分别为素数、整除、堆垒数论、丢番图方程、整数序列以及一些其它问题。

应该指出，由于本书成稿大部分在七年前，虽然这次改写尽了全力，但仍会有挂一漏万之处，特别是在本书即将出版之际，国内外许多新的问题与结果正在不断涌现，现已没有精力增写这部分内容，也不可能跟上这样一种步伐。

我由衷地感谢对本书的出版给予支持、帮助的各界朋友。黑龙江省省长田凤山在任哈尔滨市市长时就给予明确指示，尽快出版此书。哈尔滨市科委、轻工局对本书的出版均给予了支持与帮助。当时在哈尔滨工业大学读研究生的江卫民和唐虎林二位同志，在本书原稿的编译过程中自始至终给予了极大的帮助，尤其是江卫民同志，在翻译初稿和抄稿上协助做了大量的工作，借此机会一并向他们致以诚挚的感谢！

曹珍富

于哈尔滨 1994.5.20

目　录

A 素数

我们把正整数分成三类：

单位数：1

素数：2，3，5，7，11，13，17，19，23，29，31，37，…

合数：4，6，8，9，10，…

如果一个大于1的数仅有的正约数是1和它本身，便称这个数为素数；否则称为合数. Euclid 证明了素数个数无限，因此，至少从 Euclid 起，素数就已经引起了数学家的兴趣.

通常用 p_n 表示第 n 个素数，如 $p_1 = 2, p_2 = 3, p_{99} = 523$，用 $\pi(x)$ 表不超过 x 的素数个数，例如 $\pi(2) = 1, \pi(3.5) = 2, \pi(1000) = 168$. m,n 的最大公约数($g.c.d$)用(m,n)表示，如果$(m,n) = 1$，则称 m,n 互素.

Dirichlet 证明了，当 $(a,b) = 1$ 时，算术级数

$$a, a+b, a+2b, a+3b, \cdots$$

中有无限多个素数. Schinzel 和 Sierpinski 曾写过一篇综述素数问题的文章，其中给出了大量的参考文献.

在本书问题 D23 的表 7 中给出了小于 1000 的素数表.

许多世纪以来，一直吸引着许多数论家注意的问题是：怎样确定一个大数是素数还是合数？如果是合数，那么它的因子又是什么？随着高速计算机的出现，这一问题已取得了可观的进展，而密码分析的需要又更进一步促进了它的发展.

本书中我们总用 c 表示正常数，用$\langle x \rangle$表示不小于 x 的最小整数，而用$[x]$表示不大于 x 的最大整数.

[1]Leonard Adleman and Frank Thomson Leighton, An $O(n^{1/10.89})$primality

testing algorithm, *Math. Comp.*, 36(1981), 261-266.

[2]R. P. Brent, An improved Monte Carlo factorization algorithm, *BIT*, 20 (1980), 176-184.

[3]曹珍富(Z. Cao),公钥密码学,黑龙江教育出版社,1993.

[4]John D. Dixon, Asymptotically fast factorization of integers, *Math. Comp.*, 36(1981), 255-260.

[5]Richard K. Guy, How to factor a number, *Congressus Numerantiun XVI* Proc. 5th Manitoba Conf. Numer. Math., Winnipeg, 1975, 49-89.

[6]H. W. Lenstra, Primality testing. *Studieweek Getaltheorie en Computers*, Stichting Mathematisch Centrum, Amsterdam, 1980, 41-60.

[7]G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci*, 13(1976), 300-317.

[8]J. M. Pollard, Theorems on factorization and primality testing, *Proc. Cambridge Philos. Soc*, 76(1974), 521-528.

[9]J. M. Pollard, A Monte Carlo method for factorization, *BIT*, 15(1975), 331-334, *MR* 50#6992.

[10]R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications A. C. M*, Feb. 1978.

[11]A. Schinzel and W. Sierpinski, Sur certains hypotheses concernant les nombres premiers, *Acta Arith.*, 4 (1958) 185-208 (erratum5 (1959) 259); *MR* 21#4036.

[12]R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput*, 6(1977), 84-85; erratum 7 (1978), 118; *MR* 57#5885.

[13]H. C. Williams, Primality testing on a computer, *Ars Combin.*, 5(1978), 127-185; *MR* 80d: 10002.

[14]H. C. Williams and R. Holte, Some observations on primality testing, *Math. Comp.*, 32(1978), 905-917; *MR* 57#16184.

[15]H. C. Williams and J. S. Judd, Some algorithms for prime testing using generalized Lehmer functions, *Math Comp.*, 30(1976), 867-886.

A1. 二次函数的素数值

形如 a^2+1 的素数有无限多吗? Hardy 和 Littlewood(他们的猜想 E)猜测：比 n 小的这样的素数个数 $p(n)$ 渐近于 $c\sqrt{n}/\ln n$，即 $p(n)\sim c\sqrt{n}/\ln n$，就是说，当 $n\to\infty$ 时，$p(n)$ 与 $\sqrt{n}/\ln n$ 的比值趋于一个常数 c，这个常数是：

$$c=\prod_p\{1-\frac{(\frac{-1}{p})}{p-1}\}=\prod_p\{1-\frac{(-1)^{(p-1)/2}}{p-1}\}\approx 1.3727$$

其中，$(\frac{-1}{p})$ 是 Legendre 符号(见 F5)，且 $\prod_p$ 取遍所有奇素数. 对用更一般的二次表达式表示的素数个数，它们俩作了类似的猜想，唯一的差别只是 c 值不同. 但是，我们不知道一般的次数大于 1 的整值多项式(一次多项式已证明可取无穷多个素数)如何，甚至对每一个 $b>0$ 是否都有一个形如 a^2+b 的素数也没有解决.

Iwaniec 已证明，存在无穷多个 n，使 n^2+1 至多为两个素数的乘积. 他的结果可推到另外一些不可分解的二次多项式上.

Ulam 和其他人注意到，当整数序列按方螺旋形式(参见图 1)

421	420	**419**	418	417	416	415	414	413	412	411	410	**409**	408	407	406	405	404	403	402
422	**347**	346	345	344	343	342	341	340	339	338	**337**	336	335	334	333	332	**331**	330	**401**
423	348	**281**	280	279	278	**277**	276	275	274	273	272	**271**	270	**269**	268	267	266	329	400
424	**349**	282	**223**	222	221	220	219	218	217	216	215	214	213	**212**	**211**	210	265	328	399
425	350	**283**	224	**173**	172	171	170	169	168	**167**	166	165	164	**163**	162	209	264	327	398
426	351	284	225	174	**131**	130	129	128	**127**	126	125	124	123	122	161	208	**263**	326	**397**
427	352	285	226	175	132	**97**	96	95	94	93	92	91	90	121	160	207	262	325	396
428	**353**	286	**227**	176	133	98	**71**	70	69	68	**67**	66	**89**	120	159	206	261	324	395
429	354	287	228	177	134	99	72	**53**	52	51	50	65	88	119	158	205	260	323	394
430	355	288	**229**	178	135	100	73	54	**43**	42	49	64	87	118	**157**	204	259	322	393
431	356	289	230	**179**	136	**101**	74	55	44	**41**	48	63	86	117	156	203	258	321	392
432	357	290	231	180	**137**	102	75	56	45	46	**47**	62	85	116	155	201	**257**	320	**391**
433	358	291	232	**181**	138	**103**	76	57	58	**59**	60	**61**	84	115	154	201	256	319	390
434	**359**	292	**233**	182	**139**	104	77	78	**79**	80	81	82	**83**	114	153	200	255	318	**389**
435	360	**293**	234	183	140	105	106	**107**	108	**109**	110	111	112	**113**	152	**199**	254	**317**	388
436	361	294	235	184	141	142	143	144	145	146	147	148	**149**	150	**151**	198	253	316	387
437	362	295	236	185	186	187	188	189	190	**191**	192	**193**	194	195	196	**197**	252	315	386
438	363	296	237	238	**239**	240	**241**	242	243	244	245	246	247	248	249	250	**251**	314	385
439	364	297	298	299	300	301	302	303	304	305	306	307	308	309	310	**311**	312	**313**	384
440	365	366	**367**	368	369	370	371	372	**373**	374	375	376	377	378	**379**	380	381	382	**383**

图 1. 素数(黑体字)形成的对角线型

写出时，素数形成的图形似乎是一些对角线，每一对角线对应一个特定的含素数丰富的二次多项式. 例如，图 1 的主对角线与 Euler 的著名多项式 $n^2 - n + 41$ 相对应. Rabinovitch 和陆洪文发现了更一般的事实，这些事实由类数 1 的虚或实的二次域决定，例如 Euler 多项式是 Rabinovitch 的特例，陆洪文的多项式为 $N^2 - n - n^2$，这里 $N > 1$ 使得二次域 $Q(\sqrt{4N^2+1})$ 的类数为 1. 例如 $N = 13$ 符合要求，故当 $n = 1,2,\cdots,12$ 时 $169 - n - n^2$ 均是素数.

[1] Martin Gardner, The remarkable lore of prime numbers, *Scientific Amer.*, 210#3(Mar. 1964), 120-128.

[2] G. H. Hardy and J. E. Littlewood, Some problems of 'partitio numerorum' III: on the expression of a number as a sum of primes, *Acta Math.*, 44(1922), 1-70.

[3] Henryk Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.*, 47(1978), 171-188; *MR* 58#5553.

[4] 陆洪文(H. Lu)，关于实二次域的类数，科学通报，24(1979)，4:149—150.

[5] Carl Pomerance, A note on the least prime in an arithmetic progression, *J. Number Theory*, 12(1980), 218-223.

A2. 与阶乘有关的素数

形如 $n! + 1$ 的素数是否有无限多个？当 $n \leqslant 230$ 时，使 $n! + 1$ 为素数的 n 值仅仅是 1，2，3，11，27，37，41，73，77，116 和 154. 形如 $n! - 1$ 或 $x = 1 + \prod_{i=1}^{k} p_i$ 的素数是否也为无限多个？当 $p_k \leqslant 1031$ 时，x 为素数的仅有的 p_k 值是 2，3，5，7，11，31，379，1019 和 1021.

设 q 是大于 x 的最小素数，R. F. Fortune 猜想，对于所有的 k，$q - x + 1$ 是素数. 显然，它不能被前 k 个素数除尽. Selfridge 注意到，Fortune 猜想的真实性依赖于 Schinzel 的一个猜想，即，对 $x > 8$，在 x 和 $x + (\ln x)^2$ 间总存在一个素数. 目前已知的 $q - x + 1$ 形的数都是素数，它们随 $k = 1,2,3,\cdots$ 分别是 3，5，7，13，23，17，19，

23,37,61,67,61,71,47,107,59,61,109,89,103,79,… 因此，很可能 Fortune 猜测的答案是“对”. 但是，短时期内在计算机或分析工具力所能及的范围内，这种的猜测的证明仍似乎是不可想象的.

有希望解决但仍然很困难的是下面的 Erdös 和 Stewart 猜想：$1!+1=2, 2!+1=3, 3!+1=7, 4!+1=5^2, 5!+1=11^2$ 是 $n!+1=p_k^a p_{k+1}^b$ 且 $p_{k-1}\leqslant n<p_k$ 的仅有的几种情形吗？[注意，在上述五种情形里，$(a,b)=(1,0),(1,0),(0,1),(2,0)$ 和 $(0,2)$]

Erdös 又问，是否存在无穷多个素数 p，对每一个 $k(1\leqslant k!<p)$ 均有 $p-k!$ 是合数？例如，对 $p=101$ 和 $p=211$，$p-k!(1\leqslant k<p)$ 都是合数. 他认为下面的一个问题也许更易于证明：是否有无穷多个整数 $n(l!<n\leqslant(l+1)!)$，其所有素因子均大于 l，且所有 $n-k!(1\leqslant k\leqslant l)$ 是合数.

David Silverman 注意到，当 $m=1,2,3,4$ 和 8 时，乘积 $\prod_{i=1}^{m}\frac{p_i+1}{p_i-1}$ 是整数，他问是否还有其它的 m 使上述乘积为整数.

[1]I. O. Angell and H. J. Godwin, Some factorizations of $10^n\pm1$, *Math. Comp.*, 28(1974), 307-308

[2]Alan Borning, Some results for $k!\pm1$ and $2\cdot3\cdot5\cdots p\pm1$, *Math. Comp.*, 26(1972), 567-570.

[3]Martin Gardner, Mathematical Games, *Sci. Amer.*, 243#6(Dec. 1980), 18-28.

[4]S. Kravitz and D. E. Penney, An extension of Trigg's table, *Math. Mag.*, 48(1975), 92-96.

[5]Mark Templer, On the primality of $k!+1$ and $2*3*5*\cdots*p+1$, *Math. Comp.*, 34(1980), 303—304.

A3. Mersenne 素数与 Fermat 数

人们对具有特定形式的素数一直抱有兴趣，特别是对与完全数(见 B1)相联系的 Mersenne 素数 2^p-1(这里 p 必然是素数，但不

是充分条件！例如，$2^{11}-1=2047=23\times 89$)，以及 Repunit 素数 $(10^p-1)/9$.

借助于计算机及在使用计算机时用一些更为复杂的技术，Lucas—Lehmer 试验不断地增加着，得到这样一个素数表(对素数表中的每一个 p，2^p-1 也是素数)：2，3，5，7，13，17，19，31，61，89，107，127，521，607，1279，2203，2281，3217，4253，4423，9689，9941，11213，19937，21701，23209，44497，86243，132049，216091，… 无疑地，他们的个数将会是无穷多. 但是，要证明它却毫无希望. 假定 $M(x)$ 是素数 $p\leqslant x$ 使 2^p-1 为素数的个数. 对 $M(x)$ 的大小，我们希望找到一个令人信服的直观推断. Gillies 认为 $M(x)\sim c\ln x$. 但有些人不相信它.

D. H. Lehmer 置 $S_1=4$，$S_{k+1}=S_k{}^2-2$，假定 2^p-1 是一个 Mersenne 素数，注意到 $S_{p-2}\equiv 2^{(p+1)/2}$ 或 $-2^{(p+1)/2}(\bmod\ 2^p-1)$，他问：$S_{p-2}\equiv 2^{(p+1)/2}(\bmod\ 2^p-1)$ 还是 $S_{p-2}\equiv -2^{(p+1)/2}(\bmod\ 2^p-1)$？

Selfridge 猜测，如果 n 是形如 $2^k\pm 1$ 或 $2^{2k}\pm 3$ 的素数，那么，2^n-1 和 $(2^n+1)/3$ 两者要么全是素数，要么全不是. 此外，如果 2^n-1 和 $(2^n+1)/3$ 都是素数，那么 n 便具有 $2^k\pm 1$ 或 $2^k\pm 3$ 的形式之一. 一个新的 Mersenne 猜想是，如果下面三条中两条是正确的，那么第三条也正确：(a)$n=2^k\pm 1$ 或 $n=4^k\pm 3$；(b)2^n-1 是素数；(c)$(2^n+1)/3$ 是素数. 这个新猜想对于 $n<10^5$ 是正确的(参见[4]). Mullin 推广了这个猜想. 设 P，Q 是两个互素的非零整数，$P^2-4Q\neq 0$，再设 a，b 是方程 $x^2-Px+Q=0$ 的两个根，定义 $u_n=(a^n-b^n)/(a-b)(n\geqslant 0)$，$v_n=(a^n+b^n)/(a+b)(n$ 奇)，则 Mullin 提出的更一般猜想是，如果下面三条中两条是正确的，那么第三条也是正确的：(a)$n=2^k\pm 1$ 或 $4^k\pm 3$；(b)u_n 是一个素数；(c)v_n 是一个素数.

如果 p 是素数，那么 2^p-1 总是无平方因子吗？这似乎又是一个不可回答的问题. 回答“不”是安全的. 如果你运气的话，这个问题

也许能由计算机解出. 正如 D. H. Lehmer 在谈到各种分解方法时所说的:"机遇恰在角落周围徘徊."Selfridge 正确地以一个问题表述上面那个问题计算上的困难性:"试找到 50 或更多个象 1093 和 3511 的素数"(这两个素数 p 是仅有的比 3×10^9 小且它们平方能除尽 2^p-2 的素数).

与 $(10^p-1)/9$ 是素数对应的 p 值已知的有 2,19,23,317,1031,最后两个是 Hugh Williams 最近发现的. 大于 1 的 Repunit 数决不可能是平方数和立方数,这可由 Ljunggren 关于丢番图方程 $\frac{x^n-1}{x-1}=y^q$ 的结果立即推出. 但是,我们不知道什么时候它们是无平方因子数.

Fermat 数 $F_n=2^{2^n}+1$ 也一直是人们感兴趣的. 对于 $0\leqslant n\leqslant 4$,F_n 均是素数,对于 $5\leqslant n\leqslant 19$ 和许多更大的 n,F_n 为合数. Hardy 和 Wright 给出了一个直观的推断:Fermat 数中仅有有限个是素数. Selfridge 更支持如下猜想:所有其他的 Fermat 数全为合数. 王元(1979)指出:F_{14} 是目前未知其任何素因子的最大复合数.

由于形如 $k2^n+1$ 的数极有可能成为 Fermat 数的因子,因此,它们也受到了特别的注意,至少对 k 较小时是如此. 例如,Hugh Williams 发现,如果 $k=5$,那么 $n=3313$,4678 和 5947 时,$k\cdot2^n+1$ 是素数,且第一个能除尽 F_{3310}. 另外,Richard Brent 已证明,$p=1238926361552897$ 除尽 F_8 (参见 B19).

我们不大可能确切知道 Fibonacci 序列:

1,1,2,3,5,8,13,21,34,55,89,144,233,377,610,987,1597,…

(其中 $u_1=u_2=1,u_{n+1}=u_n+u_{n-1}$)$(n\geqslant2)$ 是否包含有无穷多个素数. 类似地,对于相关的 Lucas 序列:1,3,4,7,11,18,29,47,76,123,199,322,521,843,1364,…和其他更多的由二次递推关系式定义的 Lucas-Lehmer 序列 $((u_1,u_2)=1)$,情况是否也是如此呢? 但是,Graham 已证明,Lucas-Lehmer 序列当:

$u_1=1786\ 772701\ 928802\ 632268\ 715130\ 455793$

$u_2 = 1059\ 683225\ 053915\ 111058\ 165141\ 686995$

时，它不含有任何素数.

Raphael Robinson 考察了 Lucas 序列 $u_0 = 0, u_1 = 1, u_{n+1} = 2u_n + u_{n-1} (n \geqslant 1)$，并且定义了本原部分 L_n，这里 L_n 满足

$$u_n = \prod_{d|n} L_n,$$

他注意到 $L_7 = 13^2, L_{30} = 31^2$，因此，他问是否存在 $n > 30$ 使 L_n 是一个平方数.

[1]George E. Andrews, Some formulae for the Fibonacci sequence with generalizations, *Fibonacci Quart.*, 7(1969), 113-130; *MR* 39#4088.

[2]R. C. Archibald, *Scripta Math.*, 3(1935), 117.

[3]Robert Baillie, New primes of the form $k \cdot 2^n + 1$, *Math. Comp.*, 33 (1979), 1333-1336; *MR* 80h: 10009.

[4]P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr., The new Mersenne conjecture, *Amer. Math. Monthly*, 96(1989), 2: 125—128.

[5]Richard P. Brent, Factorization of the eighth Fermat number, *Abstracts Amer. Math. Soc.*, 1(1980), 565.

[6]Richard P. Brent and J. M. Pollard, Factorization of the eighth Fermat number, *Math. Comp.*, 36(1981).

[7]John Brillhart, D. H. Lehmer and J. L. Selfridge. New primality criteria and factorzations of $2^m \pm 1$, *Math. Comp.*, 29(1975), 620-627; *MR* 52# 5546.

[8]J. Brillhart, J. Tonascia and P. Weinberger, On the Fermat quotient, in A. O. L. Atkin and B. J. Birch (eds.) *Computers in Number Theory*, Academic Press, London, 1971, pp. 213-222.

[9]曹珍富(Z. Cao), On the diophantine equation $ax^2 + by^2 = p^z$, *J. Harbin Inst. Tech.*, 26(1991), 6: 108—111; *MR* 94a: 11041.

[10]Martin Gardner, Mathematical games: The strong law of small numbers, *Sci. Amer.*, 243#6(Dec. 1980), 18-28.

[11]Donald B. Gillies, Three new Mersenne primes and a statistical theory, *Math. Comp.*, 18(1964), 93-97.

[12]Gary B. Gostin, A factor of F_{17}, *Math. Comp.*, 35(1980), 975-976.

[13]R. L. Graham, A. Fibonacci-like sequence of composite numbers, *Math. Mag.*, 37(1964), 322-324.

[14]John C. Hallyburton and John Brillhart, Two new factors of Fermat numbers, *Math. Comp.*, 29(1975), 109-112; *MR* 51 # 5460. Corrigendum 30(1976), 198; *MR* 52#13599.

[15]M. Kraitchik, *Sphinx*, 1931, 31.

[16]D. H. Lehmer, *Sphinx*, 1931, 32, 164.

[17]E. Lucas, Théorie des fonctions numériques simplements périodiques, *Amer. J. Math.*, 1(1878), 184-240, 289-321(esp. p. 316).

[18]G. Matthew and H. C. Williams, Some new primes of the form $k \cdot 2^n + 1$, *Math. Comp.*, 31(1977), 797-798; *MR* 55#12605.

[19]Michael A. Morrison and John Brillhart, A method of factoring and the factorization of F_7, *Math. Comp.*, 29(1975), 183-205.

[20]Albert A. Mullin, Letter to the editor: "The new Mersenne conjecture" [Amer. Math. Monthly 96(1989), no. 2, 125—128; MR 90c: 11009] by P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr., *Amer. Math. Monthly*, 96(1989), 6: 511.

[21]Curt Noll and Laura Nickel, The 25th and 26th Mersenne primes, *Math. Comp.*, 35(1980), 1387-1390.

[22]Rudolf Ondrejka, Primes with 100 or more digits, *J. Recreational Math.*, 2(1969), 42-44; Addenda, 3(1970), 161-162; More on large primes, 11(1979), 112-113; *MR* 80g: 10012.

[23]R. E. Powers, *Amer. Math. Monthly*, 18(1911), 195-197; *Proc. London Math. Soc.* (2)13(1919), 39.

[24]Raphael M. Robinson, A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers, *Proc. Amer. Math. Soc.*, 9(1958), 673-681; *MR* 20#3097.

[25]D. E. Shippee, Four new factors of Fermat numbers, *Math. Comp.*, 32(1978), 941.

[26] David Slowinski, Searching for the 27th Mersenne prime, *J. Recreational Math.*, 11(1978-79), 258-261; *MR* 80g: 10013.

[27]C. L. Stewart, The greatest prime factor of $A^n - B^n$, *Acta Arith.*, 26 (1975), 427-433.

[28]C. L. Stewart, Divisor properties of arithmetical sequences, PhD. thesis, Cambridge, 1976.

[29]Bryant Tuckerman, The 24th Mersenne prime, *Proc. Nat. Acad. Sci. U.S.A.*, 68(1971), 2319-2320.

[30]D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly*, 67(1960), 525-532; *MR* 22#10945.

[31]王元(Y. Wang),《数论导引》附录,科学出版社,1979.

[32]H. C. Williams, Some primes with interesting digit patterns, *Math. Comp.*, 32(1978), 1306-1310; *MR* 58#484; *Zbl*. 388. 10007.

[33]H. C. Williams and E. Seah, Some primes of the form $(a^n-1)/(a-1)$, *Math. Comp.*, 33(1979), 1337-1342; *MR* 80g:10014.

[34]Samuel Yates, The mystique of repunits, *Math. Mag.*, 51 (1978), 22-28; *MR* 80f:10008.

A4. 同余类中的素数

如果正整数 b 整除 $a-c$,那么我们说,a 与 c 对模 b 同余,且记作 $a \equiv c \pmod b$. S. Chowla 猜想,如果 $(a,b)=1$,那么存在无穷多对相邻素数 p_n, p_{n+1},使 $p_n \equiv p_{n+1} \equiv a \pmod b$. 从 Littlewood 定理可知有 $b=4, a=1$ 的情形成立,且此时相邻素数出现的范围已经给出. 而当 $b=4, a=3$ 时, Knapowski 和 Turán 也给出相邻素数出现的范围. Turán 注意到,寻找相邻素数$\equiv 1 \pmod 4$的长序列将是有益的(比如,与 Riemann 假设联系起来看). Den Haan 找到了 9 个这样的相邻素数: 11593, 11597, 11617, 11621, 11633, 11657, 11677, 11681, 11689. 下面一个更长的序列有 11 个素数:

766261, 766273, 766277, 766301, 766313, 766321, 766333, 766357, 766361, 766369, 766373.

Turán 特别地对素数属性感兴趣. 设 $\pi(n;a,b)$ 是素数 $p<n$, $p\equiv a \pmod b$ 的个数,那么对于$(a,b)=1$ 的每一对 a,b,存在无穷多个 n

值，使$\pi(n;a,b)>\pi(n;a_1,b)$对于每一个$a_1 \not\equiv a(\bmod b)$均成立吗？Knapowski 和 Turán 解决了一些特殊的情形，但是，对于一般情形，该问题仍有待人们去解决.

对于$\pi(n;a,b)$，1950 年，Linnik 证明了存在c，如果$n=b^c$，那么$\pi(n;a,b)>0$. 这里的c称为 Linnik 常数. 现在的问题是：c能取多大？显然c取得越小越好. 1959 年，潘承洞首次定出$c \leqslant 5448$，1977 年 Jutila 证明了$c \leqslant 60$，后又改进为$c \leqslant 36$. 陈景润证明了$c \leqslant 17$，后又改进为$c \leqslant 15$. 这是目前最好的结果（参见[11]）.

$\pi(n;a,b)$与偶数n表为两奇素数和的表法个数密切相关（参见C1）.

Chebyshev 注意到$\pi(n;1,3)<\pi(n;2,3)$和$\pi(n;1,4)<\pi(n;3,4)$对n取较小的值成立. Leech，Shanks 和 Wrench 分别独立地发现$n=26861$时，有$\pi(n;1,4)>\pi(n;3,4)$. Bays 和 Hudson 发现，第一个不等式对于两个集合中的数不等号也相反，这两个集合中的每一个都含有1.5×10^8多个整数，且每个整数在$n=608981813029$与$n=610968213796$之间.

[1]Carter Bays and Richard H. Hudson, The appearance of tens of billions of integers x with $\pi_{24,13}(x)<\pi_{24,1}(x)$ in the vicinity of 10^{12}, *J. reine angew. Math.*, 299/300(1978), 234-237; *MR* 57#12418.

[2]Carter Bays and Richard H. Hudson, Details of the first region of integers x with $\pi_{3,2}(x)<\pi_{3,1}(x)$, *Math. Comp.*, 32(1978), 571-576.

[3]Carter Bays and Richard H. Hudson, Numerical and graphical description of all axis crossing regions for the moduli 4 and 8 which occur before 10^{12}, Internat. J. Math. Sci., 2(1979), 111-119; *MR* 80h:10003.

[4]Richard H. Hudson, A common combinatorial principle underlies Riemann's formula, the Chebyshev phenomenon, and other subtle effects in comparative prime number theory I, *J. reine angew. Math.*, 313(1980), 133-150.

[5]M. Jutila, On Linnik's constant, *Math. Scand.*, 41(1977), 45—62.

[6]S. Knapowski and P. Turán, Uber einige Fragen der vergleichenden Primzahltheorie, *Number Theory and Analysis*, Plenum Press, New York, 1969, 157-171.

[7]S. Knapowski and P. Turán, On prime numbers≡1 resp. 3(mod 4), Number Theory and Algebra, Academic Press, N. Y. 1977, pp. 157-165; *MR* 57 #5926.

[8]John Leech, Note on the distribution of prime numbers, *J. London Math. Soc.*, 32(1957), 56-58.

[9]潘承洞(C. Pan),堆垒素数论的一些新结果,数学学报,9(1959),315－329.

[10]Daniel Shanks, Quadratic residues and the distribution of primes, *Math. Tables Aids Comp.*, 13(1959), 272-284.

[11]姚琦(Q. Yao),"1＋2"以后——介绍陈景润在解析数论研究中的最新成果,自然杂志,2(1981),106－108.

A5. 素数算术级数

仅由素数组成的算术级数能有多长？它们中最小素数有多大？表1列出了含有n个素数的级数$a, a+d, \cdots, a+(n-1)d$,它们是由 V. A. Golubev, E. Karst, S. C. Root, W. N. Seredinskii 和 S. Weintraub 发现的. 当然,此时公差必定使得每个不超过n的素数成为其因子(除非$n=a$). 人们猜测n可能为任意大. 如果能改进 Szemerédi 定理(见 E7),那么这个猜想就能成立.

对于更一般的情形,Erdös 猜测,如果$\{a_i\}$为任意的整数无穷序列,且$\sum 1/a_i$是发散的,那么,该序列包含任意长的算术级数. Erdös 为这一猜想的证明或找到反例提供 3000 美元的奖金.

Pomerance 把点(n, p_n)画出来得到素数图,并且证明对于每一个k,都能找到k个素数在一条直线上.

Grosswald 已证明,在下面的意义下,存在一个长的算术级数全由"准素数"组成,即存在无穷多个k项的算术级数,每一项至多是r个素数的乘积. 其中$r \leqslant [k\ln k + 0.892k + 1]$.

表1. 长的素数算术级数

n	d	a	$a+(n-1)d$	发现时间
12	11550	166601	293651	K,1967
12	13860	110437	262897	K,1967
12	13860	152947	305407	K,1967
12	30030	23143	353473	G,1958
12	30030	1498141	1829471	K,1968
12	30030	188677831	189008161	R,1969
12	30030	805344823	805675153	R,1969
12	90090	409027	1400017	S,1966
12	90090	802951	1793941	K,1969
12	90090	862397	1853387	K,1969
13	60060	4943	725663	
13	510510	766439	6892559	S,1965
14	2462460	46883579	78895559	
16	9699690	53297929	198793279	
16	223092870	2236133941	5582526991	R,1969
17	87297210	3430751869	4827507229	W,1977

当 $(l,k)=1$ 时,算术级数 $kn+l(n=1,2,\cdots)$ 中最小素数 $P(k,l)$ 应有多大?潘承洞首先指出,存在可以计算的绝对常数 c 使 $P(k,l)=O(k^c)$,陈景润证明了 $c\leqslant 168$.

[1]陈景润(J. Chen),关于算术级数中的最小素数和 $L-$ 函数零点的两个定理,中国科学,20(1977),5:383－414.

[2]P. Erdös and P. Turán, On certain sequences of integers, *J. London Math. Soc.*, 11(1936),261-264.

[3]J. Gerver, The sum of the reciprocals of a set of integers with no arith-

metic progression of k terms, *Proc. Amer. Math. Soc.*, 62(1977), 211-214.

[4]Joseph L. Gerver and L. Thomas Ramsey, Sets of integers with no long arithmetic progressions generated by the greedy algorithm, *Math. Comp.*, 33(1979), 1353-1359.

[5]V. A. Golubev, Faktorisation der Zahlen der Form $x^3 \pm 4x^2 + 3x \pm 1$, *Anz. Oesterreich. Akad. Wiss. Math.-Naturwiss. Kl.* 1969, 184-191 (see also 191-194; 297-301; 1970, 106-112; 1972, 19-20, 178-179).

[6]Emil Grosswald, Long arithmetic progressions that consist only of primes and almost primes, *Notices Amer. Math. Soc.*, 26(1979), A-451.

[7]E. Grosswald, Arithmetic progressions of arbitrary length and consisting only of primes and almost primes, *J. Reine Angew. Math.*, 317(1980), 200-208.

[8]Emil Grosswald and Peter Hagis, Arithmetic progressions consisting only of primes, *Math. Comp.*, 33(1979), 1343-1352; *MR* 80k:10054.

[9]D. R. Heath-Brown, Almost-primes in arithmetic progressions and short intervals, *Math. Proc. Cambridge Philos. Soc.*, 83(1978), 357-375; *MR* 58#10789.

[10]Edgar Karst, 12-16 primes in arithmetical progression, *J. Recreational Math.*, 2(1969), 214-215.

[11]E. Karst, Lists of ten or more primes in arithmetical progressions, *Scripta Math.*, 28(1970), 313-317.

[12]E. Karst and S. C. Root, Teilfolgen von Primzahlen in arithmetischer Progression, *Anz. Oesterreich. Akad. Wiss. Math.-Naturwiss. Kl.* 1972, 19-20(see also 178-179).

[13]潘承洞(C. Pan),论算术级数中之最小素数,科学记录新辑,1957,1:283—286.

[14]Carl Pomerance, The prime number graph, *Math. Comp.*, 33(1979), 399-408; *MR* 80d:10013.

[15]W. Sierpinski, Remarque sur les progressions arithmetiques, *Colloq. Math.*, 3(1955), 44-49.

[16]Sol Weintraub, Seventeen primes in arithmetic progression, *Math. Comp.*, 31(1977), 1030.

[17]S. Weintraub, Primes in arithmetic progression, *BIT*, 17(1977), 239-243.
[18]K. Zarankiewicz, Problem 117, *Colloq. Math.*, 3(1955), 46, 73.

A6. 算术级数中的连续素数

甚至一直有人猜测,存在任意长的连续的素数算术级数,例如251,257,263,269和1741,1747,1753,1759. Jones 等人发现了含有5个连续素数的序列$10^{10}+24493+30k(0<k\leqslant 4)$,不久以后,Lander 和 Parkin 找到了有6个连续素数的序列:$121174811+30k(0\leqslant k\leqslant 5)$. 他们又证明了,$9843019+30k(0\leqslant k\leqslant 4)$是有5个连续素数的级数中的最小级数,且在小于$3\times 10^8$时还有另外25个这样的级数,但没有其他长度为6的这样的级数.

现在,人们仍不清楚在算术级数中具有三个连续素数的集合是否有无限多个?但 S. Chowla 在不限制为连续素数时证明了这个问题的回答是肯定的.

[1]S. Chowla, There exists an infinity of 3-combinations of primes in A. P., *Proc. Lahore Philos. Soc.* 6 (1944), no. 215-16. *MR*7, 243.
[2]P. Erdős and A. Renyi, Some problems and results on consecutive primes, *Simon Stevin*, 27(1950), 115-125; *MR*11, 644.
[3]M. F. Jones, M. Lal and W. J. Blundon, Statistics on certain large primes, *Math. Comp.*, 21(1967), 103-107; *MR* 36 # 3707.
[4]L. J. Lander and T. R. Parkin, Consecutive primes in arithmetic progression, *Math. Comp.*, 21(1967), 489.

A7. Cunningham 链

证明p是素数的一个普通方法涉及到$p-1$的分解,如$p-1=2q$,其中q是另一个素数,那么,这个问题的规模便减少了1/2. 因此,观察一下素数的 Cunningham 链是非常有趣的:该链后一项是紧邻的前项的2倍加1. D. H. Lehmer 发现仅有三条这样的链,各

有7个素数.链中最小的数$<10^7$:

1122659,2245319,4490639,8981279,17962559,35925119,71850239;

2164229,4328459,8656919,17313839,34627679,69255359,138510719;

2329469,4658939,9317879,18635759,37271519,74543039,149086079.

他还找到起始数为10257809和10309889的另外二条链. $p+1$ 的分解也能被用来证明 p 是素数.Lehmer 基于 $p+1=2q$ 找到7条长度为7的链.头三条链的起始值分别为16651,67651和165901.已知不存在长度为8的链.Lehmer 估计,在6或7百万次试算中,大概可能有一次能找到一条起始数在10^9附近的链.

[1]D. H. Lehmer,Tests for primality by the converse of Fermat's theorem, *Bull. Amer. Math. Soc.*, 33(1927),327-340.

[2]D. H. Lehmer, On certain chains of primes, *Proc. London Math. Soc.*, 14A(Littlewood 80 volume,1965),183-186.

A8. 相邻素数之差

有许多问题都与相邻素数的区间有关,记 $d_n=p_{n+1}-p_n$,因此有 $d_1=1$,且所有其他的 d_n 都是偶数.那么 d_n 能有多大?并且 d_n 是多少?Rankin 已证明:

$$d_n>\frac{c\ln n\ln\ln n\ln\ln\ln\ln n}{(\ln\ln\ln n)^2}$$

对无穷多个 n 成立. Erdös 为常数 c 可取任意大的证明或找到的反例提供10,000美元的奖金.Rankin 的最好结果是 $c=e^\gamma$,其中 γ 为 Euler 常数.

最著名的一个猜想是孪生素数猜想,即 $d_n=2$ 有无穷多个.陈景润(1973)证明了:有无限多个素数 p,使 $p+2$ 为不超过 2 个素数之积. Hardy 和 Littlewood 的猜想 B 是,小于 n 且差为偶数 k

的素数对的个数 $p_k(n)$ 为：

$$p_k(n) \sim \frac{2cn}{(\ln n)^2} \prod \frac{p-1}{p-2},$$

其中，乘积取遍 k 的所有奇素因子（因此，$k=2$ 时，乘积取 1)，且 $c = \prod (1-1/(p-1)^2)$，$\prod$ 取遍所有奇素数. 因而 $2c \approx 1.32032$. Lehmer 和 Riesel 独立地发现了大孪生素数 $9 \times 2^{211} \pm 1$. 最近，Crandall 和 Penk 又发现了有64，136，154，203和303位的孪生素数. Williams 找到 $156 \times 5^{202} \pm 1$，Baillie 找到 $297 \times 2^{546} \pm 1$. Atkin 和 Rickert 又找到孪生素数对 $694513810 \times 2^{2304} \pm 1$ 与 $1159142985 \times 2^{2304} \pm 1$. Parady 和 Smith 找到了已知的最大三对新孪生素数 $663777 \times 2^{7650} \pm 1$，$571305 \times 2^{7701} \pm 1$ 和 $1706595 \times 2^{11235} \pm 1$.

Bombieri 和 Davenport 已经证明：

$$\lim_{n \to \infty} \frac{d_n}{\ln p_n} \leqslant \frac{2+\sqrt{3}}{8} \approx 0.46650$$

（无疑，真正的答案为零. 当然，如果孪生素数猜想的真实性得到确认则将推导出这一点). Huxley 已证明，$d_n < p_n^{7/12+\epsilon}$. 并且 Heath-Brown 和 Iwaniec 最近已把上述结果改进为 $d_n < p_n^{11/20+\epsilon}$. Cramer 用 Riemann 假设证明了，$\sum_{n \leqslant x} d_n^2 < cx(\ln x)^4$. Erdős 猜测，上述不等式右边应为 $cx(\ln x)^2$. 但是，他同时认为，没有希望证明这一点. Riemann 假设蕴含 $d_n < p_n^{1/2+\epsilon}$.

Shanks 已给出了一个直观的推断支持下述猜想：如果 $p(g)$ 是跟在 g 或更多个合数形成的区间后的第一个素数，那么 $\ln p(g) \sim \sqrt{g}$. Lehmer 把所有小于 37×10^6 的素数制成一个表，从下页表2中知，在素数20831323和20831533之间有209个合数，即 $g = 209$. Lander 和 Parkin 继续这一工作，找到 $g < 314$. Brent 继续到 $g < 534$. 表 2 中，对应于 $g = 381$ 和 651 项的 p_{n+1} 值是 $p(g)$. Weintraub 已经找到 1.1×10^{16} 附近的区间值 $g = 653$.

陈景润(1979)已证明，对于充分大的 x 和任意的 $\alpha \geqslant 0.477$，在区间 $[x, x+x^\alpha]$ 内必存在一个数，它至多是两个素数的积. 有一

表 2. 若干相邻素数间的间隔

g	p_n	p_{n+1}	发现者
209	20831323	20831533	*Lehmer*
219	47326693	47326913	*Parkin*
221	122164747	122164969	*Lander & Parkin*
233	189695659	189695893	*Lander & Parkin*
281	436273009	436273291	*Lander & Parkin*
291	1453168141	145318433	*Lander & Parkin*
381	10726904659	10726905041	*Lander & Parkin*
463	42652618343	42652618807	*Brent*
533	614487453523	614487454057	*Brent*
601	1968188556461	1968188557063	*Brent*
651	2614941710599	2614941711251	*Brent*

个著名的猜想没有解决：在 n^2 与 $(n+1)^2$ 之间一定存在素数. 显然，如证明在 $[x, x+x^\alpha]$ $(\alpha \geqslant 0.5)$ 内存在素数，则上述猜想被证明. 现在只能证明当 $\alpha > 0.55$ 时，对充分大的 x，$[x, x+x^\alpha]$ 中存在素数.

[1]A. O. L. Atkin and N. W. Rickert, On a larger pair of twin primes, Abstract 79T-A132, *Notices Amer. Math. Soc.*, 26(1979), A-373.

[2]Robert Baillie, New primes of the form $k \cdot 2^n + 1$, *Math. Comp.*, 33 (1979), 1333-1336.

[3]E. Bombieri and H. Davenport, Small differences between prime numbers, *Proc. Roy. Soc.* Ser. A, 293(1966), 1-18; *MR* 33#7314.

[4]Richard P. Brent, The first occurrence of large gaps between successive primes, *Math. Comp.*, 27(1973), 959-963; *MR* 48#8360(and see 35 (1980), 1435-1436).

[5] J. H. Cadwell, Large intervals between consecutive primes, *Math. Comp.*, 25(1971), 909-913.

[6]陈景润(J. Chen)，大偶数表为一个素数与一个不超过两个素数的乘积之和，中国科学，16(1973)，2:111－128.

[7]陈景润(Jing-Run Chen), On the distribution of almost primes in an inter-

val II, *Sci. Sinica*, 22(1979), 253-275; *Zbl* 408. 10030.

[8]R. J. Cook, On the occurrence of large gaps between prime numbers, *Glasgow Math. J.*, 20(1979), 43-48; *MR* 80e:10034.

[9]Harald Cramer, On the order of magnitude of the difference between consecutive prime numbers, *Acta Arith.*, 2(1937), 23-46.

[10]R. E. Crandall and M. A. Penk, A search for large twin prime pairs, *Math. Comp.*, 33(1979), 383-388; *MR* 81a:10010.

[11]D. R. Heath-Brown, The difference between consecutive primes, *J. London Math. Soc.*, (2)18(1978), 7-13; 19(1979), 207-220; 20(1979), 177-178; *MR* 58#10787; 80k:10041; 81f:10055.

[12]D. R. Heath-Brown and H. Iwaniec, On the difference between consecutive primes, *Inventiones Math.*, 55(1979), 49-69; *MR* 81h:10064; see also *Bull. Amer. Math. Soc.*, (N. S)1(1979), 758-760; *MR* 80d:10064.

[13]Martin N. Huxley, The difference between consecutive primes, *Proc. Symp. Pure Math. Amer. Math. Soc.*, 24(Analytic Number Theory, St. Louis, 1972), 141-145; *MR* 50#9816.

[14]Martin N. Huxley, On the difference between consecutive primes, *Invent. Math.*, 15(1972), 164-170.

[15]M. N. Huxley, A note on large gaps between prime numbers, *Acta Arith.*, 38(1980), 63-68.

[16]M. N. Huxley, Small differences between consecutive primes I, *Mathematika*, 20(1973),, 229-232; *MR* 50#4509; II, 24(1977), 142-152; *MR* 57#5925.

[17]Aleksandar Ivic, On sums of large differences between consecutive primes, *Math. Ann.*, 241(1979), 1-9; *MR* 80i:10057.

[18]Henryk Iwaniec and Matti Jutila, Primes in short intervals, *Ark. Mat.*, 17(1979), 167-176; *Zbl.* 408. 10029.

[19]L. J. Lander and T. R. Parkin, On first appearance of prime differences, *Math. Comp.*, 21(1967), 483-488; *MR* 37#6237.

[20]D. H. Lehmer, Table concerning the distribution of primes up to 37 millions, 1957, deposited in UMT file, reviewed in *Math. Tables Aids Comp.*, 13(1959), 56-57.

[21]B. K. Parady, Joel F. Smith, and Sergio E. Zarantonello, Largest known twin primes, *Math. Comp.*, 55(1990), 191; 381—382.

[22]R. A. Rankin, The difference between consecutive primes, *J. London Math. Soc.*, 13 (1938), 242-247; II *Proc. Cambridge Philos. Soc.*, 36 (1940), 255-266; *MR* 1-292; III *J. London Math. Soc.*, 22(1947), 226-230; *MR*9-498; IV *Proc. Amer. Math. Soc.*, 1(1950), 143-150; *MR* 11-644; V *Proc. Edinburgh Math. Soc.* (2) 13(1962-63), 331-332; *MR* 28 #3978.

[23]H. Riesel, Lucasian criteria for the primality of $N = h \cdot 2^n - 1$, *Math. Comp.*, 23(1969), 869-875.

[24]Daniel Shanks, On maximal gaps between successive primes, *Math. Comp.*, 18(1964), 646-651; *MR* 29# 4745.

[25]Sol Weintraub, A large prime gap, *Math. Comp.*, 36(1981), 279.

[26]H. C. Williams, Primality testing on a computer, *Ars Combinatoria*, 5 (1978), 172-185.

[27]H. C. Williams and C. R. Zarnke, A report on prime numbers of the form $M = (6a + 1)2^{2m-1} - 1$ and $M' = (6a - 1)2^{2m} - 1$, *Math. Comp.*, 22 (1968), 420-422.

[28]D. Wolke, Grosse Differenzen zwischen aufeinanderfolgenden Primzahlen, *Math. Ann.*, 218(1975), 269-271; *MR* 56# 11930.

A9. 类型中素数个数

比孪生素数猜想更一般的猜想是这样的：假如不用同余关系来消除它们，那么任何给定类型的素数集合都有无穷多个. 例如有无穷多个三个一组的素数集合 $\{6k - 1, 6k + 1, 6k + 5\}$ 和 $\{6k + 1, 6k + 5, 6k + 7\}$ 似乎是正确的，它的证明要比孪生素数猜想困难，但它的似是而非却具有很大的吸引力，而且 Hensley 和 Richards 已经证明，下面的猜想不能和它相容，即对于所有的整数 $x, y \geq 2$，

$$“\pi(x + y) \leqslant \pi(x) + \pi(y)”$$

这里，我们之所以放了引号，是因为它极有可能是错的. 实际上，有

希望找到与它相矛盾的 x,y 值. 但是,还有一个替代猜想:

$$\pi(x+y) \leqslant \pi(x) + 2\pi(y/2).$$

此时 Hensley—Richards 的方法无法对它进行评论了.

H. F. Smith 注意到,在素数序列11,13,17,19,23,29,31,37中,后一项与前项的差序列为2,4,2,4,6,2,6. 至少有三个素数序列是这样的差序列,其起始数分别为15760091,25658841和93625991. 但在这三种情形里,与41对应的项都不是素数. 当 $n=88830$ 和 855750 时,$n-11, n-13, \cdots, n-41$ 都为素数,但 $n-43$ 不是素数, John Leech 注意到,找到33个比11大的连续整数,其中包含有10个素数这一问题仍未解决. 更一般地,找到 n 个数的集合,在此集合中,同余条件不影响它至少含有 $\pi(n)$ 个素数.

[1]Paul Erdös and Ian Richards, Density functions for prime and elatively prime numbers, *Monatsh. Math.*, 83(1977), 99-112; Zbl. 355. 10034.

[2]Douglas Hensley and Ian Richards, On the incompatibility of two conjectures concerning primes, *Proc. Symp. Pure Math. Amer. Math. Soc.*, 24 (Analytic Number Theory, St. Louis, 1972), 123-127.

[3]Ian Richards, On the incompatibility of two conjectures concerning primes, a discussion of the use of computers in attacking a theoretical problem, *Bull. Amer. Math. Soc.*, 80(1974), 419-438.

[4]Herschel F. Smith, On a generalization of the prime pair problem, *Math. Tables Aids Comput.*, 11(1957), 249-254.

A10. Gilbreath 猜想

我们用 $d_n^1 = d_n, d_n^{k+1} = |d_{n+1}^k - d_n^k|$ 来定义 d_n^k(见下页图2). N. L. Gilbreath 猜想,对于所有 $k, d_1^k = 1$. Killgrove 和 Ralston 已证明了 $k < 63419$ (即素数<792722)时猜想成立.

人们认为,关于这个专题已弄得过分神秘了,其实,它与素数本身没有什么关系. 但是,对任何由2和奇数组成的序列猜想是正确的. 这些奇数以"有理"速率增加,并且具有"有理"大小的区间.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89

1 2 2 4 2 4 2 4 6 2 6 4 2 4 6 6 2 6 4 2 6 4 6

1 0 2 2 2 2 2 2 4 4 2 2 2 2 0 4 4 2 2 4 2 2

1 2 0 0 0 0 0 2 0 2 0 0 0 2 4 0 2 0 2 2 0

1 2 0 0 0 0 2 2 2 2 0 0 2 2 4 2 2 2 0 2

1 2 0 0 0 2 0 0 0 2 0 2 0 2 2 0 0 2 2

1 2 0 0 2 2 0 0 2 2 2 2 2 0 2 0 2 0

1 2 0 2 0 2 0 2 0 0 0 0 2 2 2 2 2

1 2 2 2 2 2 2 2 0 0 0 2 0 0 0 0

1 0 0 0 0 0 0 2 0 0 2 2 0 0 0

图2. 素数序列的逐次绝对差

[1]R. B. Killgrove and K. E. Ralston, On a conjecture concerning the primes, *Math. Tables Aids Comput.*, 13(1959), 121-122; *MR* 21#4943.

A11. 相邻素数差的增加和减小

因为素数占的比例逐渐减少，因此虽然不一定每一次必有 $d_m < d_{m+1}$，但它却出现无穷多次. Erdős 和 Turán 已经证明，$d_n > d_{n+1}$ 也是如此. 他们还证明了使 $d_n > d_{n+1}$ 成立的 n 值具有正下密率. 但是，现在仍不知道是否存在无穷多个由三个递增或递减的相邻的 d_n 组成的集合. 如没有，那么，存在 n_0 使得对每一个 i 和 $n > n_0$，我们都有 $d_{n+2i} > d_{n+2i+1}$ 和 $d_{n+2i+1} < d_{n+2i+2}$ 吗？Erdős 为证明这样的 n_0 不存在提供了 100 美元的奖金.

[1]P. Erdős, On the difference of consecutive primes, *Bull. Amer. Math. Soc.*, 54(1948), 885-889; *MR* 10, 235.

[2]P. Erdős and P. Turán, On some new questions on the distribution of prime numbers, *Bull. Amer. Math. Soc.*, 54(1948), 371-378; *MR* 9, 498.

A12. **几种伪素数**

Pomerance，Selfridge 和 Wagstaff 称满足 $a^{n-1}\equiv 1 \pmod n$ 的奇合数 n 为以 a 为基的伪素数(记为 $psp(a)$)，从而避免了大量文献中出现的不适用的"复合伪素数"概念. 如果对每一与 n 互素的 a，奇合数 n 都是 $psp(a)$，那么称 n 为 Carmichael 数. 又如果对于任意奇合数 n 有 $(a,n)=1$，且 $a^{(n-1)/2}\equiv\left(\frac{a}{n}\right) \pmod n$，那么称它为以 a 为基的欧拉伪素数(记为 $epsp(a)$)，其中 $\left(\frac{a}{n}\right)$ 是雅可比符号(见F5). 最后，如果奇合数 n 满足 $n-1=2^s\cdot d$，d 奇数，且 $a^d\equiv 1 \pmod n$ (否则，对某些 r，$a^{d\cdot 2^r}\equiv -1 \pmod n$，其中 $0\leqslant r<s$)，则称它为以 a 为基的强伪素数(记为 $spsp(a)$). 这些定义全可由 Venn 图来说明(图3). 图3还给出了每一集合中的最小元素.

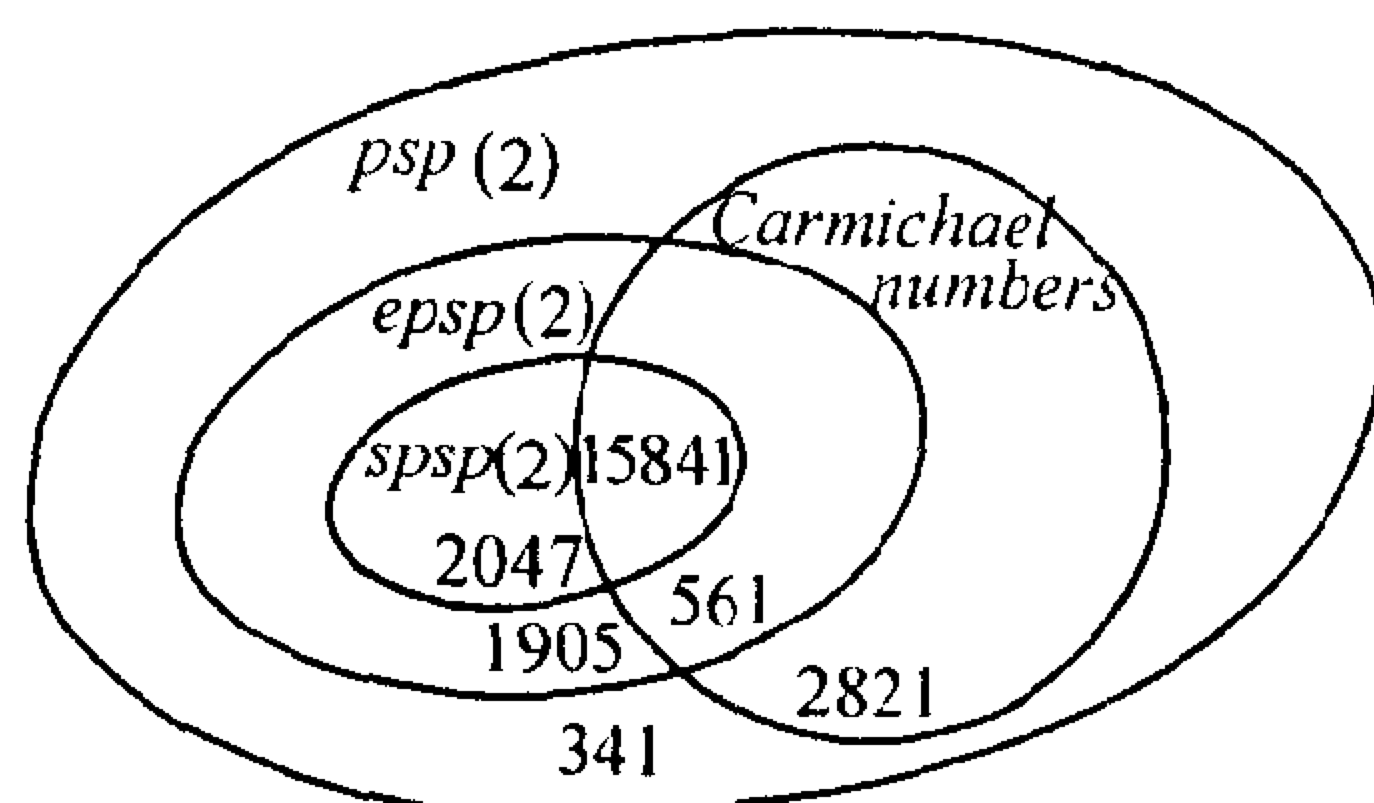


图3. 伪素数集合的关系及每一个集合中的最小元素

下表中的 $P_2(x)$，$E_2(x)$，$S_2(x)$ 和 $C(x)$ 分别表小于 x 的 $psp(2)$，$epsp(2)$，$spsp(2)$ 和 Carmichael 数的个数，其数值是由 Pomerance，Selfridge 和 Wagstaff 共同给出的：

x	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	2.5×10^{10}
$P_2(x)$	3	22	78	245	750	2057	5597	14884	21853
$E_2(x)$	1	12	36	114	375	1071	2939	7706	11347
$S_2(x)$	0	5	16	46	162	488	1282	3291	4842
$C(x)$	1	7	16	43	105	255	646	1547	2163

Lehmer 和 Erdös 证明了

$$c_1 \ln x < P_2(x) < x \exp\{-c_2(\ln x \ln\ln x)^{1/2}\},$$

而最近，Pomerance 把界改进到：

$$\exp\{(\ln x)^{5/14}\} < P_2(x) < x \exp\{(-\ln x \ln\ln\ln x)/2\ln\ln x\}$$

并且他猜测，真实的估计应是：

$$\exp\{(\ln x)^{5/14}\} < P_2(x) < x \exp\{(-\ln x \ln\ln\ln x)/\ln\ln x\}.$$

偶 $psp(2)$ 也是存在的. 例如，Lehmer 找到一个，$161038=2\times 73\times 1103$，而 Beeger 证明了有无穷多个. 如果 F_n 是 Fermat 数 $2^{2^n}+1$，且如果 $k>1, n_1<n_2<\cdots<n_k<2^{n_1}$，则 Cipolla 证明了 $F_{n_1}F_{n_2}\cdots F_{n_k}$ 是 $psp(2)$.

如果 $P_n^{(a)}$ 是第 n 个 $psp(a)$，Szymiczek 证明了 $\sum 1/P_n^{(2)}$ 是收敛的. 而 Makowski 证明了 $\sum 1/\ln P_n^{(a)}$ 是发散的. Rotkiewicz 列出了关于伪素数的58个问题和20个猜想.

[1]N. G. W. H. Beeger, On even numbers m dividing 2^m-2, *Amer. Math. Monthly*, 58(1951), 553-555; *MR* 13, 320.

[2]R. D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1}\equiv 1 \bmod P$, *Amer. Math. Monthly*, 19(1912), 22-27.

[3]M. Cipolla, Sui numeri composti P che verificiano la congruenza di Fermat, $a^{P-1}\equiv 1 (\bmod P)$, *Annali di Matematica*, 9(1904), 139-160.

[4]P. Erdös, On the converse of Fermat's theorem, *Amer. Math. Monthly*, 56(1949), 623-624; *MR* 11, 331.

[5]P. Erdös, On almost primes. *Amer. Math. Monthly*, 57(1950), 404-407; *MR* 12, 80.

[6]D. H. Lehmer, On the converse of Fermat's theorem, *Amer. Math. Monthly*, 43(1936), 347-354; II, 56(1949), 300-309; *MR* 10, 681.

[7]Andrzej Makowski, On a problem of Rotkiewicz on pseudoprime numbers, *Elem. Math.*, 29(1974), 13.

[8]A. Makowski and A. Rotkiewicz, On pseudoprime numbers of special form, *Colloq. Math.*, 20(1969), 269-271; *MR* 39#5458.

[9]Carl Pomerance, John L. Selfridge, and Samuel S. Wagstaff, The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.*, 35(1980), 1003-1026.
[10]A. Rotkiewicz, *Pseudoprime Numbers and their Generalizations*, Student Association of the Faculty of Sciences, Univ. of Novi Sad, 1972; *MR* 48#8373; *Zbl*. 324.10007.
[11]A. Rotkiewicz, Sur les diviseurs composés des nombres $a^n - b^n$, *Bull. Soc. Roy. Sci*. Liége, 32(1963), 191-195; *MR* 26# 3645.
[12]A. Rotkiewicz, Sur les nombres pseudopremiers de la forme $ax + b$, *Comptes Rendus Acad. Sci. Paris*, 257(1963), 2601-2604; *MR* 29#61.
[13]A. Rotkiewicz, Sur les formules donnant des nombres pseudopremiers, *Colloq. Math.*, 12(1964), 69-72; *MR* 29#3416.
[14]A. Rotkiewicz, Sur les nombres pseudopremiers de la forme $nk + 1$, *Elem. Math.*, 21(1966), 32-33; *MR* 33#112.
[15]K. Szymiczek, On prime numbers p, q and r such that pq, pr and qr are pseudoprimes, *Colloq. Math.*, 13(1964-65), 259-263; *MR* 31#4757.
[16]K. Szymiczek, On pseudoprime numbers which are products of distinct primes, *Amer. Math. Monthly*, 74(1967), 35-37; *MR* 34#5764.

A13. Carmichael 数

Carmichael 数(见 A12)必定是无平方因子数且至少含有三个素因子，如 $561 = 3 \times 11 \times 17$. 但我们不知道是否存在无穷多个 Carmichael 数. Erdös 猜测，当 $x \to \infty$ 时，$\frac{(\ln C(x))}{\ln x} \to 1$，$C(x)$ 表小于 x 的素数个数. 他改进了 Knödel 的一个结果并证明了：

$$C(x) < x \exp(-c \ln x \ln \ln \ln x / \ln \ln x).$$

而同时 Pomerance, Selfridge 和 Wagstaff(见 A12)也证明了上述结果，只是 $c = 1 - \varepsilon$. 并且，他们给出了支持此猜想的直观推断，即当 $c = 2 + \varepsilon$ 时，

$$C(x) > x\exp(-c \ln x \ln \ln \ln x / \ln \ln x)$$

成立.

J. R. Hill 已找到一个巨大的 Carmichael 数为 pqr，其中 $p = 5$

$\times 10^9 + 371, q = 10^{20} + 741$ 和 $r = 1 + (p-1)(q+2)/433$. Pomerance, Selfridge 和 Wagstaff, Jr. 已经找到所有小于 25×10^9 的 Carmichael 数. 最近, Jaeschke 计算了 25×10^9 至 10^{12} 的所有 Carmichael 数, 共6075个.

[1] Robert Baillie and Samuel S. Wagstaff, Lucas pseudoprimes, *Math. Comp.*, 35(1980), 1391-1417.

[2] P. Erdös, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen*, 4(1956), 201-206; *MR* 18, 18.

[3] Jay Roderick Hill, Large Carmichael numbers with three prime factors, Abstract 79T-A136, *Notices Amer. Math. Soc.*, 26(1979), A-374.

[4] Gerhard Jaeschke, The Carmichael numbers to 10^{12}, *Math. Comp.*, 55 (1990), 191: 383—389.

[5] W. Knödel, Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x, *Arch. Math.*, 4(1953), 282-284; *MR* 15. 289.

[6] D. H. Lehmer, Strong Carmichael numbers, *J. Austral. Math. Soc.* Ser. A, 21(1976), 508-510.

[7] C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr. *Math. Comp.*, 35 (1980), 151: 1003—1026.

[8] A. J. van der Poorten and A. Rotkiewicz, On strong pseudoprimes in arithmetic progressions, *J. Austral. Math. Soc.* Ser. A, 29 (1980), 316-321.

[9] S. S. Wagstaff, Large Carmichael numbers, *Math. J. Okayama Univ.*, 22 (1980), 33-41.

[10] H. C. Williams, On numbers analogous to Carmichael numbers, *Canad. Math. Bull.*, 20(1977)133-143.

[11] M. Yorinaga, Numerical computation of Carmichael numbers, *Math. J. Okayama Univ.*, 20(1978), 151-163; *MR* 80d: 10026.

A14. 好素数

Erdös 和 Straus 称素数 p_n 为好的, 如果 $p_n^2 > p_{n-i}p_{n+i}$ 对于所有 $i(1\leqslant i\leqslant n-1)$ 成立. 例如: 5, 11, 17, 29 是好素数. Pomerance

用“素数图”(见 A5)证明了有无穷多个好素数,并提出下面几个问题:使 p_n 为好素数的 n 的集合的密率为零吗?存在无穷多个 n 使 $p_n p_{n+1} > p_{n-i} p_{n+1+i}$ 对所有 $i(0 < i < n)$ 成立吗?存在无穷多个 n 使 $p_n + p_{n+1} < p_{n-i} + p_{n+1+i}$ 对所有 $i(0 < i < n)$ 成立吗?对所有 $i(0 < i < n)$ 使 $2p_n < p_{n-i} + p_{n+i}$ 成立的 n 的集合,其密率为0吗(Pomerance 已证明了有无穷多个这样的 n)?又 $\limsup(\min\limits_{0<i<n}(p_{n-i} + p_{n+i}) - 2p_n) = \infty$ 吗?

A15. 连续数乘积的同余

1979年,Erdös 发现:$3\times4\equiv5\times6\times7\equiv1(\bmod 11)$,并问使

$$\prod_{i=1}^{k_1}(a+i)\equiv\prod_{i=1}^{k_2}(a+k_1+i)$$
$$\equiv\prod_{i=1}^{k_3}(a+k_1+k_2+i)\equiv1(\bmod p)$$

成立的最小素数 p 是什么?这里 a,k_1,k_2,k_3 是整数.他认为,对任意个上述同余乘积式,这样的素数都存在.

A16. Gauss 素数与 Eisenstein 素数

除了有理域外,素数还能定义在其他域上.在复数域上,它们被称为 Gauss 素数.普通素数问题可重新对 Gauss 素数进行阐述.

从存在唯一分解的角度看,Gauss 整数 $a+bi$(其中 a,b 是整数,$i^2=-1$)似乎有点象普通整数(仅除了序、单位(±1, $\pm i$)以及相伴数:如 7 的相伴数 $7,-7,7i$ 和 $-7i$ 以外).形如 $4k-1$ 的素数仍为 Gauss 素数(3,7,11,19,23,…),但是,另外的普通素数则不然,因为它可分解为 Gauss 素数的积,如:

$2=(1+i)(1-i)$,

$5=(2-i)(2+i)=-(2i-1)(2i+1)$,等等,

$13=(2+3i)(2-3i)$,$17=(4+i)(4-i)$,

$29=(5+2i)(5-2i)$,…

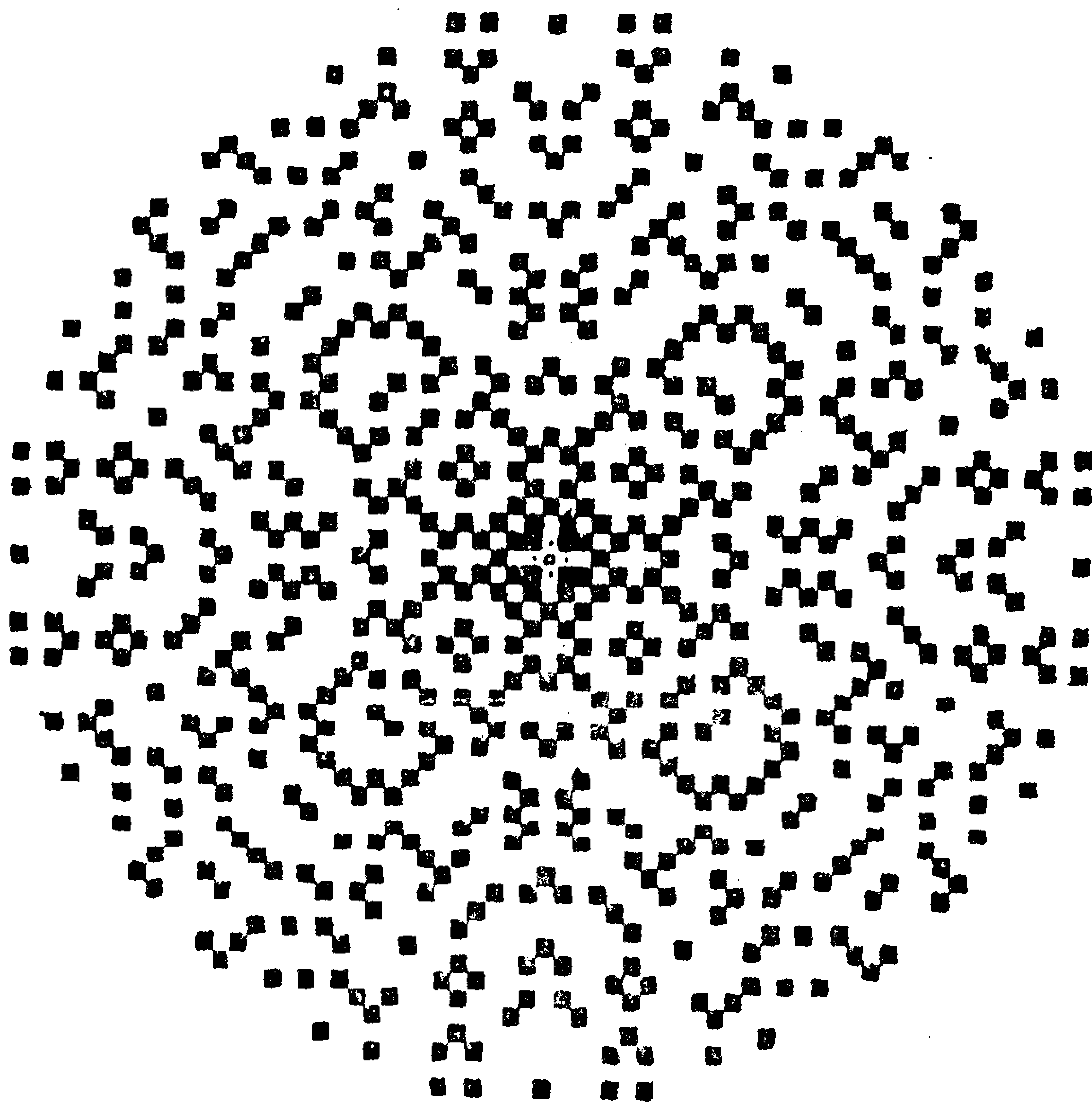


图 4. 范数小于 1000 的 Gauss 素数

当我们把 Gauss 素数 $\pm 1 \pm i$, $\pm 2 \pm i$, $\pm 3i$, $\pm 2 \pm 3i$, $\pm 4 \pm i$, $\pm 5 \pm 2i$, …画在 Argand 图上时,结果它们形成了一幅令人愉悦的图案(见图4). 这些图案在给地板贴瓷砖和制蜡染桌布时已被人们采用.

Motzkin 和 Gordon 问,人们能否以高斯素数为"踏脚石",以边界长为步距从起点"走"到无穷?这大概不可能. Jordan 和 Rabung 已证明步距至少是4.

Eisenstein 整数 $a + b\omega$ 具有唯一的分解,其中 a,b 是整数,ω

是1的复三次单位根且满足$\omega^2+\omega+1=0$,这些素数再次形成一图形,因为有6个单位数± 1, $\pm\omega$, $\pm\omega^2$,因此图形是对称六边形,素数2和形如$6k-1$(5,11,17,23,29,41,…)的素数仍然是Eisenstein素数,但素数3和形如$6k+1$的那些素数能被分解,如:

$$3=(1-\omega)(1-\omega^2),7=(2-\omega)(2-\omega^2),$$

$$13=(3-\omega)(3-\omega^2),19=(3-2\omega)(3-\omega^2),$$

$$31=(5-\omega)(5-\omega^2),37=(4-3\omega)(4-3\omega^2),\cdots$$

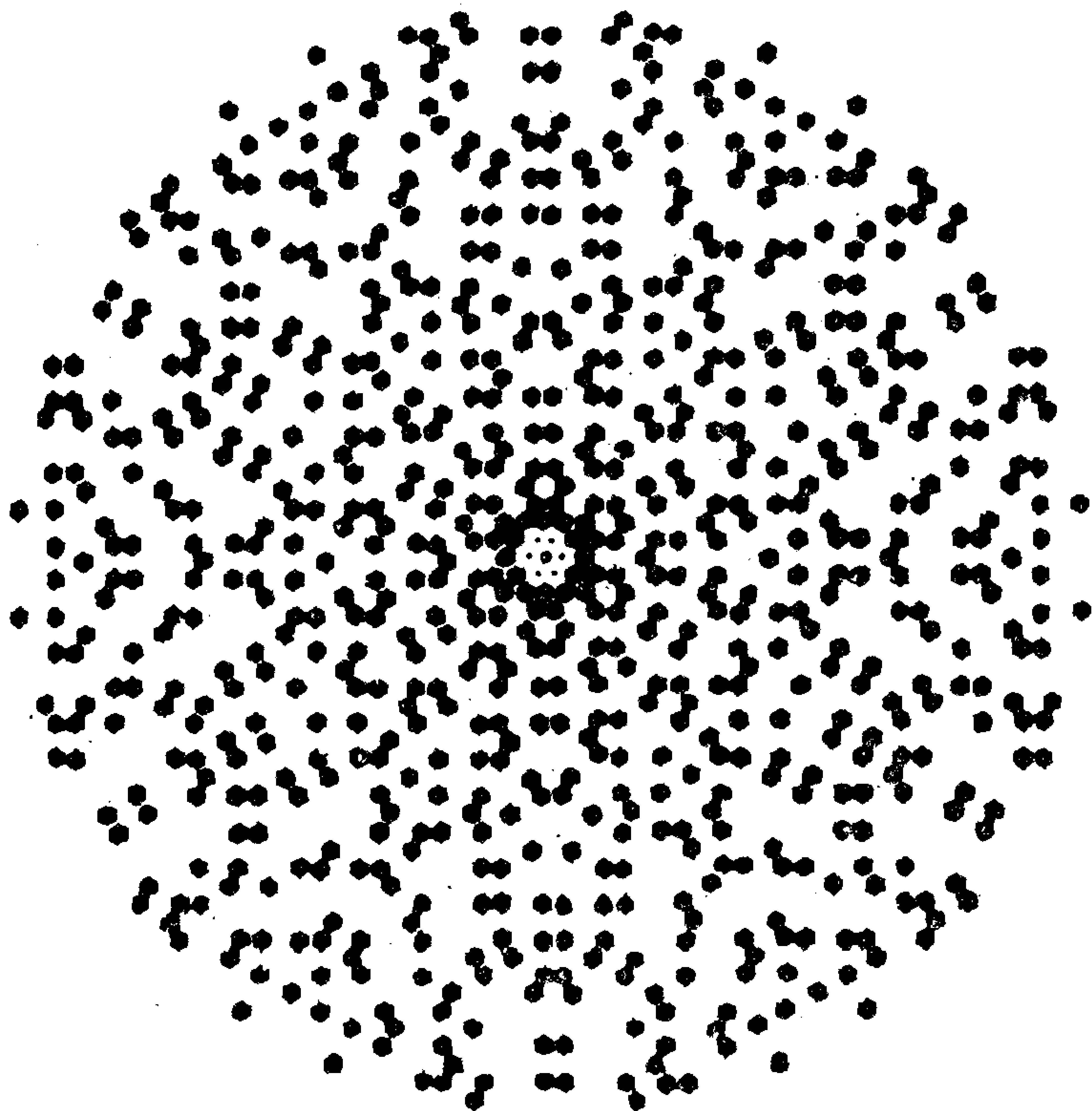


图5. Eisenstein 素数

在含有复三次单位根的域上,Eisenstein素数被描绘成图5,与这

些素数对应的问题也能重新阐述.

Eisenstein 素数已经被用来设计密码体制,那么,距很大的两个 Eisenstein 素数的乘积能以多快的速度分解?对 Gauss 素数的相应问题如何?

[1]曹珍富(Z. Cao),公钥密码学,第四章§4.3,黑龙江教育出版社,1993.

[2]曹珍富(Z. Cao),Z[ω]环上的两类密码体制,电子科学学刊,14(1992),286-290.

[3]J. H. Jordan and J. R. Rabung, A conjecture of Paul Erdös concerning Gaussian primes, *Math. Comp.*, 24(1970),221-223.

A17. 素性的充要条件

Wilson 定理是:p 是素数的充分必要条件是 $(p-1)!+1 \equiv 0 \pmod p$. C. P. Willans 和 C. P. Wormell 用它得到关于 p_n, $\pi(x)$ 或素性的充要条件的一些公式,且仅用到初等函数,但是太繁琐了,此处无法刊出. Matjasevic 和其他逻辑学家用 Wilson 定理解决了 Hilbert 第十问题. 那么,存在能替代 Wilson 定理的类似结论吗?

Sierpinski 注意到,从 Fermat 定理可得出,如果 p 是素数,则 $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}+1\equiv 0 \pmod p$, 那么逆命题成立吗?Giuga 证明了 $p\leqslant 10^{1000}$ 时逆命题成立,康继鼎和周国富证明了逆命题仅当 p 为素数或 $p=\prod_{j=1}^{n} p_j$ 成立,其中 $p_j(j=1,\cdots,n)$ 为不同的奇素数,$n>100$, 且 $p_1\cdots p_{j-1}p_{j+1}\cdots p_n\equiv 1(\mathrm{mod}\, p_j(p_j-1))(j=1,\cdots,n)$. 曹珍富猜想,对任意 n 个奇素数 $p_j(j=1,\cdots,n)$, $p_1\cdots p_{j-1}p_{j+1}\cdots p_n\equiv 1(\mathrm{mod}\, p_j(p_j-1))(j=1,\cdots,n)$ 不成立,因而前述逆命题成立.

[1]L. E. Dickson, *History of the Theory of Numbers*, G. E. Stechert & Co, New York, 1934, Vol. I, Chap. XVIII.

[2] G. Giuga, Sopra alcune proprieta caratteristiche dei numeri primi, *Period. Math.* (4) 23(1943), 12-27; *MR* 8,11.

[3] Giuseppe Giuga, Su una presumibile proprieta caratteristica dei numeri primi, *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat.* (3) 14 (83) (1950), 511-528; *MR* 13,725.

[4] 康继鼎(J. D. Kang), 周国富, 关于居加猜想与费马数为素数的充要条件, 数学通报, 12(1981), 20—22.

[5] W. Sierpinski, *Elementary Number Theory*, p. 205.

[6] C. P. Willans, On formulae for the *N*th prime number, *Math. Gaz.*, 48 (1964), 413-415.

[7] C. P. Wormell, Formulae for primes, *Math. Gaz.*, 51(1967), 36-38.

A18. 一个素数同余式组

如果 $p_j(j=1,\cdots,n)$ 是奇素数，则 $2p_1\cdots p_{j-1}p_{j+1}\cdots p_n+1\equiv 0(\mathrm{mod}\,p_j)(j=1,\cdots,n)$ 成立吗？柯召和孙琦已经证明在 $1\leqslant n\leqslant 5$ 时均仅有一组素数 $p_j(j=1,\cdots,n)$ 满足同余式组，即有：

$n=1:p_1=3$;

$n=2:p_1=3,p_2=7$;

$n=3:p_1=3,p_2=7,p_3=43$;

$n=4:p_1=3,p_2=11,p_3=23,p_4=31$;

$n=5:p_1=3,p_2=11,p_3=23,p_4=31,p_5=47059$.

同时，柯召和孙琦还猜想，对每个 n，同余式组最少有一组解. 曹珍富，刘锐和张良瑞借助于计算机证明了 $n=6$ 时，同余式组也仅有一组解，即 $p_1=3,p_2=11,p_3=17,p_4=101,p_5=149,p_6=3109$. 因此，他们猜想同余式组最多有一组解.

[1] 曹珍富(Z. Cao), R. Liu and L. Zhang, On the Equation $\sum_{j=1}^{s}(1/x_j)+(1/(x_1\cdots x_s))=1$ and Znam's Problem, *J. Number Theory*, 27(1987), 206-211.

[2] 柯召(Chao Ko), 孙琦, 关于单位分数表1的问题, 四川大学学报(自然科

学版),1(1964),13—29.

A19. Erdös-Selfridge 对素数数的分类

Erdös 和 Selfridge 将素数分类如下：如果 $p+1$ 仅有素因子 2 或 3，则 p 为第 1 类；如果 $p+1$ 的每一个素因子属于 $\leqslant r-1$ 的各类素数中，则 p 为第 r 类，其中等号至少对于一个素因子成立. 例如：

第1类　2 3 5 7 11 17 23 31 47 53 71 107 127 191 431 647 863 971 …

第2类　13 19 29 41 43 59 61 67 79 83 89 97 101 109 131 137 139 149 167 179 197 199 211 223 229 239 241 251 263 269 271 281 283 293 307 317 319 359 367 373 377 383 419 439 449 461 467 499 503 509 557 563 577 587 593 599 619 641 643 659 709 719 743 751 761 769 809 827 839 881 919 929 953 967 979 991 …

第3类　37 103 113 151 157 163 173 181 193 227 233 257 277 311 331 337 347 353 379 389 397 401 409 421 457 463 467 487 491 521 523 541 547 571 601 607 613 631 653 683 701 727 733 773 787 811 821 829 853 857 859 877 883 911 937 947 983 997 …

第4类　73 313 443 617 661 673 677 691 739 757 823 887 907 941 977 …

第5类　1021 1321 1381 …

容易证明，对任给的 $\varepsilon>0$ 和所有的 r，不超过 n 的第 r 类中素数个数为 $o(n^{\varepsilon})$. 但不知道每一类中是否有无穷多个素数. 如 $p_1^{(r)}$ 表第 r 类中的最小素数，则 $p_1^{(1)}=2, p_1^{(2)}=13, p_1^{(3)}=37, p_1^{(4)}=73$ 和 $p_1^{(5)}=1021$. Erdös 猜想 $(p_1^{(r)})^{1/r}\to\infty$. 但 Selfridge 认为它极可能是有界的.

如果用 $p-1$ 代替 $p+1$，并且仿上类似的分类，则上面相应

的问题如何？

[1]P. Erdős, Problems in Number Theory and Combinatorics, *Congressus Numerantium XVIII*, Proc. 6th Conf. Numerical Math., Manitoba, 1976, 35-58(esp. p. 53); *MR* 80e:10005.

A20. 取 n 使 $n-2^k$ 为素数等

Erdős 猜想7,15,21,45,75和105是仅有的 n 值，它使对所有满足 $2\leqslant 2^k<n$ 的 k，$n-2^k$ 是素数. Mientka 和 Weitzenkamp 已证明了 $n<2^{44}$ 时猜想为真. Vaughan 利用 Montgomery 筛法也给出了一个估计.

Erdős 又猜想，对无穷多个 n，所有的整数 $n-2^k(1\leqslant 2^k<n)$ 是无平方因子数(参见 F12).

Cohen 和 Selfridge 问不为 $\pm p^a\pm 2^b$ 形的最小正奇数是什么，其中 p 为素数，$a\geqslant 0, b\geqslant 1$，且式中±号可任取. 他们注意到该数 $>2^{18}$，但认为它至多为

6120 6699060672 7677809211 5601756625 4819576161-
6319229817 3436854933 4512406741 7420946855 8999326569.

Crocker 证明了存在无穷多个奇整数不为 2^k+2^l+p 的形式. Erdős 问，对每个 r 是否存在无穷多个奇整数，它不是一个素数与2的 r 或更低次幂的和？他们密率为正吗？他们含有无穷算术级数吗？另一方面，Gallagher 证明了，对任给的 $\varepsilon>0$，存在充分大的 r 使素数与 2 的 r 次幂的和之下密率 $>1-\varepsilon$.

Erdős 又问，是否存在不为 2^k+s 形式的奇整数，其中 s 是无平方因子数. 此问题与覆盖同余(见 F13)有联系.

设 $f(n)$ 是 n 表为 2^k+p 的个数，又设 $\{a_i\}$ 是使 $f(n)>0$ 的 n 值序列，那么 $\{a_i\}$ 的密率存在吗？Erdős 证明了 $f(n)>c\ln\ln n$ 对无穷多个 n 成立，但是不能肯定是否 $f(n)=o(\ln n)$. 他猜想：

$$\limsup(a_{i+1}-a_i)=\infty.$$

如果存在有任意大的最小模覆盖系，那么该猜想成立.

Carl Pomerance 注意到对 $n=210$，对于所有 $7<p<n$，$n-p$ 为素数，他问是否存在其他满足上述关系的 n？

[1]Fred Cohen and J. L. Selfridge, Not every number is the sum or difference of two prime powers, *Math. Comp.*, 29(1975), 79-81.

[2]R. Crocker, On the sum of a prime and of two powers of two, *Pacific J. Math.*, 36(1971), 103-107; *MR* 43#3200.

[3]P. Erdős, On integers of the form 2^r+p and some related problems, *Summa Brasil. Math.*, 2(1947-51), 113-123; *MR* 13, 437.

[4]Patrick X. Gallagher, Primes and powers of 2, *Inventiones Math.*, 29 (1975), 125-142.

[5]W. E. Mientka and R. C. Weitzenkamp, On f-plentiful numbers, *J. Combin. Theory*, 7(1969), 374-377.

[6]A. de Polignac, Recherches nouvelles sur les nombres premiers, *C. R. Acad. Sci. Paris*, 29(1849), 397-401, 738-739.

[7]R. C. Vaughan, Some applications of Montgomery's sieve, *J. Number Theory*, 5(1973), 64-79; *MR* 49#7222.

B 整除

我们用$d(n)$表n的正因子个数，用$\sigma(n)$表示这些因子的和，用$\sigma_k(n)$表这些因子k次幂的和，因此有$\sigma_0(n)=d(n)$，$\sigma_1(n)=\sigma(n)$。我们又用$s(n)$表n的真因子的和，也即为除开n本身，n的正因子的和，因此$s(n)=\sigma(n)-n$.

各类算术函数的叠代用$s^k(n)$表示. $s^k(n)$这样定义：对$k\geqslant 0$，$s^0(n)=n$，$s^{k+1}(n)=s(s^k(n))$.

我们用符号$d|n$表d除尽n，$e\nmid n$表e除不尽n，$p^k\|n$表$p^k|n$但$p^{k+1}\nmid n$. 而且$[m,n]$表连续的整数$m,m+1,\cdots,n$.

B1. 完全数

满足$s(n)=n$的数称为完全数. Euclid 得到，如果2^p-1是素数，则$2^{p-1}(2^p-1)$是完全的. 例如，6，28，496 等(参见 A3 中的 Mersenne 素数表). Euler 证明，$2^{p-1}(2^p-1)$是仅有的偶完全数.

那么奇完全数是否存在？这是数论中的一个臭名昭著的未解决问题. Euler 首先证明：若n为奇完全数，则$n=p^a q_1^{2b_1}\cdots q_s^{2b_s}$，这里$p,q_1,\cdots,q_s$表示不同的奇素数，$a$及$b_1,\cdots,b_s$表正整数，且$p\equiv a\equiv 1\pmod 4$. Starni 证明：如果所有的$q_i\equiv 3\pmod 4$，那么$\sigma(p^a)/2$是合数；如果所有的$q_i\equiv 1\pmod 4$，那么$p\equiv a\pmod 8$. Tuckerman, Hagis, Stubblefield, Buxton 和 Elmore 已把界逐渐地推到了10^{200}，在此界下，不存在奇完全数(但人们对 Buxton 和 Elmore 的证明存有疑问). Brent, Cohen 和 te Riele 将界推到10^{300}. Hagis 和 Chein 已独立证明，奇完全数可被至少 8 个互异素数除尽.

Muskat 证明，奇完全数可以被大于10^{12}的素数幂除尽. Hagis 和 McDaniel 证明，最大的素因子大于 100110. Pomerance 证明，次

最大的素因子比 138 大. 而 Condict 和 Hagis 已把上述的界改进到 300000 和 1000. Pomerance 还证明了,至多有 k 个互异因子的奇完全数小于 $(4k)^{(4k)^{2^{k^2}}}$.

有一个未解决的问题是:两位以上的完全数,把它的各位数字加起来得一个数,再把这个数的各位数字加起来又得到一个数,一直做下去,直到得到一个一位数. 那么这个一位数一定是 1 吗?(参看[12]). 很容易证明,对偶完全数这个问题的回答是肯定的. 又由于奇完全数很可能是不存在的,所以这个问题的回答很可能是肯定的.

[1]R. P. Brent, G. L. Cohen, and H. J. J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Math. Comp.*, 57(1991), 196: 857-868; *MR* 92c:11004.

[2]M. Buxton and S. Elmore, An extension of lower bounds for odd perfect numbers, *Notices Amer. Math. Soc.*, 23(1976), A-55.

[3]E. Z. Chein, PhD thesis, Pennsylvania State Univ., 1979.

[4]E. Z. Chein, An odd perfect number has at least 8 prime factors, Abstract 79T-A102. *Notices Amer. Math. Soc.*, 26(1979), A-365.

[5]G. L. Cohen, On odd perfect numbers, *Fibonacci Quart.*, 16(1978), 523-527; *MR* 80g:10010; *Zbl.* 391.10008.

[6]Graeme L. Cohen, On odd perfect numbers (II), Multiperfect numbers and quasiperfect numbers, *J. Austral. Math. Soc.*, Ser. A, 29(1980), 369-384.

[7]G. L. Cohen and M. D. Hendy, Polygonal supports for sequences of primes, *Math. Chronicle*, 9(1980), 120-136.

[8]J. T. Condiet, On an odd perfect number's largest prime divisor, senior thesis, Middlebury College, May, 1978.

[9]G. G. Dandapat, J. L. Hunsucker, and Carl Pomerance, Some new results on odd perfect numbers, *Pacific J. Math.*, 57(1975), 359-364.

[10]L. Euler, Commentationes arithmeticae, Vol. 2, Tractatus de numerorum

doctrina(1849),514;Opera postuma,1(1862),14-15.

[11]John A. Ewell,On the multiplicative structure of odd perfect numbers, *J. Number Theory*,12(1980),339-342;*MR* 82a:10005.

[12]葛克阳(K. Ge),数学猜想和它的故事,人民教育出版社,北京,1989,p. 7.

[13]O. Grün,Über ungerade vollkommene Zahlen, *Math. Zeit.* ,55(1952), 353-354.

[14]Peter Hagis,A lower bound for the set of odd perfect numbers, *Math. Comp.* ,27(1973), 951-953.

[15]P. Hagis,Every odd perfect number has at least 8 prime factors, *Notices Amer. Math. Soc* . ,22(1975),A-60.

[16]Peter Hagis,Outline of a proof that every odd perfect number has at least eight prime factors, *Math. Comp.* ,34 (1980),1027-1032.

[17]Peter Hagis,On the second largest prime factor of an odd perfect number, *Proc. Grosswald Conf.* ,*Lecture Notes in Mathematics*, Springer-Verlag,New York,1980.

[18]Peter Hagis and Wayne McDaniel,On the largest prime divisor of an odd perfect number, *Maht. Comp.*, 27(1973), 955-957; *MR* 48#3855; II. *ibid*, 29(1975),922-924.

[19]H. -J. Kanold,Untersuchungen über ungerade vollkommene Za * hlen, *J. reine angew. Math.* ,183(1941),98-109;*MR* 3,268.

[20]P. J. McCarthy,Odd perfect numbers, *Scripta Math.* ,23(1957),43-47.

[21]Wayne McDaniel,On odd multiply perfect numbers, *Boll. Un. Mat. Ital.* ,(4)3(1970),185-190;*MR*41#6764.

[22]Wayne L. McDaniel and Peter Hagis,Some results concerning the non-existence of odd perfect numbers of the form $p^{\alpha}M^{2\beta}$,*Fibonacci Quart.* , 13(1975),25-28.

[23]Joseph B. Muskat,On divisors of odd perfect numbers, *Math. Comp.* , 20(1966),141-144;*MR* 32#4076.

[24]Karl K. Norton,Remarks on the number of factors of an odd perfect number, *Acta Arith.* ,6(1961),365-374 (and see 36(1980),163); *MR* 26#4950

[25]M. Perisastri,A note on odd perfect numbers, *Math. Stud.* ,26(1958),

179-181.

[26]C. Pomerance, Odd perfect numbers are divisible by at least seven distinct primes, *Acta Arith.*, 25(1974), 265-300; see also *Notices Amer. Math. Soc.*, 19(1972), A-622-623.

[27]C. Pomerance, The second largest factor of an odd perfect number, *Math. Comp.*, 29(1975), 914-921.

[28]Carl Pomerance, Multiply perfect numbers. Mersenne primes and effective com-putability, *Math. Ann.*, 226(1977), 195-206.

[29]N. Robbins, The non-existence of odd perfect numbers with less than seven distinct prime factors, PhD dissertation, Polytech. Inst. Brooklyn, June 1972.

[30]Hans Salié, Über abundante Zahlen, *Math. Nachr.*, 9(1953), 217-220.

[31]C. Servais, Sur les nombres parfaits, *Mathesis*, 8(1888), 92-93.

[32]Daniel Shanks, *Solved and Unsolved problems in Number Theory*, 2nd ed. Chelsea, New York 1978, esp. p. 217.

[33]Paolo Starni, On the Euler's factor of an odd perfect number, *J. Number Theory*, 37(1991), 3:366-369; *MR* 92a:11010.

[34]Bryant Tuckerman, A search procedure and lower bound for odd perfect numbers, *Math. Comp.*, 27(1973), 943-949.

B2. 相关完全数

也许是因为未能够证明奇完全数存在，许多作者定义了若干紧密相关的概念，且由此产生了大量的问题，其中许多问题似乎不比原始问题更易处理.

对于完全数 $\sigma(n) = 2n$，如果 $\sigma(n) < 2n$，则 n 称为不足数；如果 $\sigma(n) > 2n$，则 n 称为过剩数. 如果 $\sigma(n) = 2n - 1$，则 n 称为近完全数. 2 的幂是近完全的，但不知道是否还有其他的近完全数. 如果 $\sigma(n) = 2n + 1$，则 n 被称为拟完全的. 拟完全数必定是奇平方数. 但是，没有一个人知道是否存在拟完全数. Masao Kishore 证明，如果 n 是拟完全数，则 $n > 10^{30}$，且 $\omega(n) \geqslant 6$，其中 $\omega(n)$ 是 n 的不同素因子的个数. Hagis 和 Cohen 已改进此结果到 $n > 10^{35}$，$\omega(n) \geqslant 7$.

Catteneo 起初声称已证明了 $3\nmid n$，但是，Sierpinski 和其他人已经说明 Catteneo 的证明是靠不住的. Kravitz 在一封信中作出了更一般的猜测，不存在过剩数 n，使得 $\sigma(n)-2n$ 是奇平方数. 关于此，Graeme Cohen 写道，下面的结果是很有趣的：

$$\sigma(2^2 3^2 5^2) = 3(2^2 3^2 5^2) + 11^2$$

以及如果 $\sigma(n) = 2n + k^2, (n,k) = 1, \omega(n) = 3$，则 $105|n$ 或 $165|n$，且 $n > 10^{500}, k > 10^{250}$. 后来，在放宽了 $(n,k) = 1$ 的条件后，他分别地找到了解：

$$n = 2 \cdot 3^2 \cdot 238897^2, k = 3^2 \cdot 23 \cdot 1999$$

和

$$n = 2^2 \cdot 7^2 \cdot p^2, p = 53, 277, 541, 153941, 358276277,$$
$$k = 7 \cdot 29, 5 \cdot 7 \cdot 23, 5 \cdot 7 \cdot 43, 5 \cdot 7 \cdot 103 \cdot 113,$$
$$5 \cdot 7 \cdot 227 \cdot 229 \cdot 521$$

他证明，后 5 个数中的头一个是有奇平方过剩数的最小整数. Erdős 问，对于某些常数 c，使 $|\sigma(n) - 2n| < c$ 成立的大数的特征是什么？例如 $n = 2^m$；还存在其他的吗？

如果一个数是它自己一些因子的和，那么 Sierpinski 把它称为伪完全的. 例如 $20 = 1 + 4 + 5 + 10$. Erdős 已证明，它们的密率存在. 如果一个数是过剩的，但它的所有真因子都是不足的，则称此数为本原过剩的；如果一个数是伪完全的，但它的真因子却没有一个是，则称它是本原伪完全的. 如果 n 的所有因子的调和平均为整数，则 Pomerance 称它为调和数. Andreas 和 E. Zachariou 称它们为 Ore 数，且他们称本原伪完全数为不可分的半完全数. 他们注意到，一个伪完全数的倍数还是伪完全的，且伪完全数和调和数都包含完全数作为其真子集. 后一个结果归于 Ore. 所有形如 $2^m p$ 的数都是本原伪完全的，其中 $m \geqslant 1$，p 是介于 2^m 与 2^{m+1} 间的素数. 但也存在不具有上述形式的伪完全数，如 770. 另外还知道，存在无穷多个本原伪完全数不是调和数. 最小的奇本原伪完全数是 945. Erdős 能证明，奇本原伪完全数有无穷多个.

Garcia 找到了小于 10^7 的全部调和数，共 45 个. 同时还找到了比 10^7 大的 200 多个调和数. 其中除开 1 和完全数以外，最小的一个是 140. 现在的问题是除开 1 以外，它们中的任何一个是平方数吗？它们的个数有无穷多吗？如果回答是肯定的，那么对小于 x 的那些数的个数，找出上界和下界. Kanold 已证明，它们的密率为 0，并且 Pomerance 证明，形如 $p^a q^b$(p,q 是素数)的调和数是偶完全数. 如果 $n = p^a q^b r^c$ 是调和数，那么它是偶的吗？

调和数将取哪个值？大概不可能是 4，12，16，18，20，22，…；那它取 23 吗？Ore 自己猜想：每一个 Ore 数是偶数，言外之意是不存在奇完全数.

Bateman，Erdös，Pomerance 和 Straus 证明了，对于使 $\sigma(n)/d(n)$ 为整数的 n 的集合，其密率为 1；使 $\sigma(n)/d(n)^2$ 为整数的 n 的集合，其密率为 1/2，具有形式 $\sigma(n)/d(n)$ 的有理数 $r \leqslant x$ 的个数是 $o(x)$. 他们寻找 $\frac{1}{x}\sum 1$ 的渐近公式，这里和式取遍 $\leqslant x$ 且使 $d(n)$ 除不尽 $\sigma(n)$ 的所有 n. 他们猜测，使 $d(n)$ 除尽 $s(n) = \sigma(n) - n$ 的整数 n 的密率为 0. 但是，他们缺乏直接了当的证明.

Benkoski 称一个数为怪异的，如果它是过剩的但却不是伪完全的. 例如 70 不是 $1+2+5+7+10+14+35=74$ 的任何子集的和. 小于一百万的数中有 24 个本原怪异数：70，836，4030，5830，7192，…. 而非本原怪异数包括：$70p$，p 是素数，且 $p > \sigma(70) = 144$；$836p$，p 是 421，487，491 或 p 是素数且 $\geqslant 557$；7192×31. 一些大怪异数是 Kravitz 发现的，且 Benkoski 和 Erdös 证明它们的密率是正的，这里，一些未决问题是：存在无穷多个本原过剩数，它们是怪异的吗？每一个奇过剩数是伪完全的(也就是说，不是怪异的)吗？对于怪异数 n，$\sigma(n)/n$ 能是任意大吗？Benkoski 和 Erdös 猜测后一问题的回答是“不”. Erdös 对上述后两个问题的解决分别提供 10 美元和 25 美元的奖金.

如果 $\sigma(n) = kn$，则这样的数 n 被称为倍完全数或 k 重完全数.

例如,普通的完全数是 2 重完全数,120 是 3 重完全数. Dickson 的《数论的历史》已记载了人们对这样数的悠久兴趣. 已知的最大 k 值为 8. 对于这样的 k ,Brown 给出了三个例子(Franqui 和 Garcia 又给出了另外两个),它们最小的是 $2 \cdot 3^{23} \cdot 5^9 \cdot 7^{12} \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29^2 \cdot 31^2 \cdot 37 \cdot 41 \cdot 53 \cdot 61 \cdot 67^2 \cdot 71^2 \cdot 73 \cdot 83 \cdot 89 \cdot 103 \cdot 127 \cdot 131 \cdot 149 \cdot 211 \cdot 307 \cdot 331 \cdot 463 \cdot 521 \cdot 683 \cdot 709 \cdot 1279 \cdot 2141 \cdot 2557 \cdot 5113 \cdot 6481 \cdot 10429 \cdot 20857 \cdot 110563 \cdot 599479 \cdot 1648168401$. 无疑地,$k$ 能取我们希望的那样大,尽管 Erdös 猜想 $k = o(\ln \ln n)$. Hagis 和 Cohen 对 $k > 2$ 重完全数证明了其最大的两个素因子分别 $\geqslant 100129$ 和 $\geqslant 1009$;Hagis 又进一步证明第三大素因子 $\geqslant 101$.

Minoli 和 Bear 定义,如果 $n = 1 + k\sum d_i$,其中 $\sum d_i$ 是 n 的所有真因子的和,$1 < d_i < n$,则 n 称为 k 次超完全数. 显然,如果 n 是 k 次超完全数,则 $k\sigma(n) = (k+1)n + k - 1$. 例如,21,2133 和 19521 都是 2 次超完全的,325 是 3 次超完全的. 他们猜想,对于每一个 k,存在 k 次超完全数.

Graham 问,是否 $s(n) = [n/2]$ 蕴含着 n 是 2 或是 3 的幂.

Erdös 假设对于某些 k,$f(n)$ 是满足 $n = \sum_{i=1}^{t} d_i$ 的最小整数,其中,$1 < d_1 < d_2 < \cdots < d_t = f(n)$ 是 $f(n)$ 的因子的递增序列. 那么 $f(n) = o(n)$ 吗?或是它仅对"几乎所有的"n 成立吗?

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(n)$	1	-	2	3	-	5	4	7	15	12	21	6	9	13
n	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$f(n)$	8	12	30	10	42	19	18	20	57	14	36	46	30	12

[1]H. Abbott, C. E. Aull, Ezra Brown, and D. Suryanarayana, Quasiperfect numbers, *Acta Arith.*, 22(1973), 439 447; *MR*47#4915. Corrections, *ibid*, 29(1976), 427-428.

[2]M. M. Artuhov, On the problem of odd h-fold perfect numbers, *Acta*

Arith.,23(1973),249-255.

[3] P. T. Bateman, P. Erdős, C. Pomerance, and E. G. Straus, in *Proc Grosswald Conf.*,Springer-Verlag,New York,1980.

[4]S. J. Benkoski,Problem E. 2308, *Amer. Math. Monthly*,79(1972),774.

[5]S. J. Benkoski and P. Erdős,On weird and pseudoperfect numbers, *Math. Comp.*,28(1974),617-623;*MR*50# 228 (Corrigendum, S. Kravitz, *ibid.* 29(1975),673).

[6] Alan L. Brown, Multiperfect numbers, *Scripta Math.*,20(1954), 103-106;*MR* 16,12.

[7] Paolo Catteneo, Sui numeri quasiperfetti, *Boll. Un. Mat. Ital.* (3), 6(1951),59-62;*Zbl.* 42,268.

[8]G. L. Cohen and M. D. Hendy,On odd multiperfect numbers, *Math. Chronicle*,9(1980).

[9]J. T. Cross,A note on almost perfect numbers, *Math. Mag.*,47(1974), 230-231.

[10]P. Erdős,Problems in number theory and combinatorics, *Congressus Numerantium XVIII,Proc. 6th Conf. Numerical Math. Manitoba*, 1976,35-58 (esp. pp. 53-54); *MR* 80e;10005.

[11]Benito Franqui and Mariano Garcia,Some new multiply perfect numbers, *Amer. Math. Monthly*,60(1953),459-462.

[12]Benito Franqui and Mariano Garcia, 57 new multiply perfect numbers, *Scripta Math.*,29(1954),169-171(1955).

[13]Mariano Garcia,A generalization of multiply perfect numbers, *Scripta Math.*,19(1953),209-210.

[14]Mariano Garcia, On numbers with integral harmonic mean, *Amer. Math. Monthly*,61(1954),89-96.

[15]P. Hagis Jr.,The third largest prime factor of an odd multiperfect number exceeds 100, *Bull. Malaysian Math. Soc.* (2),9(1986),2;43-49.

[16]B. Hornfeck and E. Wirsing,Über die Häufigkeit vollkommener Zahlen, *Math. Ann.*,133(1957),431-438;*MR*19,837. See also *ibid*,137(1959), 316-318;*MR*21 # 3389.

[17]R. P. Jerrard and Nicholas Temperley,Almost perfect numbers, *Math.*

Mag. ,46(1973),84-87.

[18]H. -J. Kanold,Üder das harmonische Mittel der Teiler einer natürlichen Zahl, *Math. Ann.* ,133(1957),371-374 .

[19]David G. Kendall, The scale of perfection, *J. Appl. Probability*, 19 A (P. A. P. Moran birthday volume, 1982).

[20]Masao Kishore, Odd almost perfect numbers, *Notices Amer. Math. Soc.* ,22(1975), A-380.

[21]Masao Kishore, Quasiperfect numbers are divisible by at least six distinct prime factors, *Notices Amer. Math. Soc.* ,22(1975), A-441.

[22]Masao Kishore, Odd integers N with 5 distinct prime factors for which $2-10^{-12}<\sigma(N)/N<2+10^{-12}$, *Math. Comp* . ,32(1978),303-309.

[23]M. S. Klamkin, Problem E. 1445*, *Amer. Math. Monthly*, 67(1960), 1028. See also *ibid* ,82(1975)73,

[24]Sydney Kravitz, A search for large weird numbers, *J. Recreational Math.* ,9(1976-77),82-85.

[25]A. Makowski, Remarques sur les fonctions $\theta(n)$, $\varphi(n)$ et $\sigma(n)$, *Mathesis*, 69(1960),302-303.

[26]A. Makowski, Some equations involving the sum of divisors, *Elem. Math.* ,34(1979),82; *MR* 81b:10004.

[27]D. Minoli, Issues in non-linear hyperperfect numbers, *Math. Comp.* , 34(1980),639-645.

[28]Daniel Minoli and Robert Bear, Hyperperfect numbers, *Pi Mu Epsilon J.* ,6#3(1974-75),153-157.

[29]Oystein Ore, On the averages of the divisors of a number, *Amer. Math. Monthly*, 55(1948),615-619.

[30]Seppo Pajunen, On primitive weird numbers, *A collection of manuscripts, related to the Fibonacci sequence*, 18th anniv. , Fol. Gibonacci Assoc. ,162-166.

[31]Carl Pomerance, On multiply perfect numbers with a special property, *Pacific J. Math.* ,57(1975),511-517.

[32]Carl Pomerance, On the congruences $\sigma(n)\equiv a \pmod n$ and $n\equiv a \pmod{\varphi(n)}$, *Acta Arith* . , 26(1975),265-272.

[33]Paul Poulet, *La Chasse aux Nombres*, Fascicule I, Bruxelles, 1929, 9-27.
[34]Problem B-6, William Lowell Putnam Mathematical Competition, 1976; 12:04.
[35]Herman J. J. te Riele, Hyperperfect numbers with three different prime factors, *Math. Comp.*, 36(1981), 297-298.
[36]Neville Robbins, A class of solutions of the equation $\sigma(n) = 2n + t$, *Fibonacci Quart.*, 18(1980), 137-147(misprints in solutions for $t = 31$, 84, 86).
[37]H. N. Shapiro, Note on a theorem of Dickson, *Bull. Amer. Math. Soc.*, 55(1949), 450-452.
[38]H. N. Shapiro, On primitive abundant numbers, *Comm. Pure Appl. Math.*, 21(1968), 111-118.
[39]W. Sierpinski, Sur les nombres pseudoparfaits, *Mat. Vesnik*, 2(17)(1965), 212-213; *MR* 33# 7296.
[40]W. Sierpinski, *Number Theory* (in Polish), 1959, p. 257.
[41]D. Suryanarayana, Quasi-perfect numbers, II, *Bull. Calcutta Math. Soc.*, 69(1977), 421-426; *MR* 80m: 10003.
[42]Andreas and Eleni Zachariou, Perfect, semi-perfect and Ore numbers, *Bull. Soc. Math. Grece (N. S.)*, 13(1972), 12-22; *MR* 50# 12905.

B3. 酉完全数

如果 d 除尽 n，且 $(d, n/d) = 1$，则称 d 为 n 的酉因子数. 如果 n 是它的酉因子(不包括 n 自身)的和，则称其为酉完全数. 已知不存在奇酉完全数，且 Subbarao 猜想，仅存在有限个偶酉完全数. Subbarao, Carlitz 和 Erdős 每人为这一问题的解决提供 10 美元奖金. Subbarao 为每一个新例子提供 10 美分. 如果 $n = 2^a m$，其中 m 是奇的且有 r 个不同的素因子，则当 $a \leqslant 10$ 或 $r \leqslant 6$ 时，Subbarao 和其他人已证明，除开 $2 \cdot 3, 2^2 \cdot 3 \cdot 5, 2 \cdot 3^2 \cdot 5$ 和 $2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$，没有酉完全数. 而当 m 为无平方因子的奇数时，Graham 证明除 $2 \cdot 3, 2^2 \cdot 3 \cdot 5$ 和 $2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ 外，无酉完全数. Wall 已找到酉完全数：

$2^{18} \cdot 3 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 79 \cdot 109 \cdot 157 \cdot 313$
并且证明，它是第五个这样的数. Frey 已证明，如果 $N = 2^m p_1^{a_1} \cdots p_r^{a_r}$ 是酉完全的，其中$(N,3) = 1$，那么 $m > 144$，$r > 144$，$N > 10^{440}$.

Ligh 和 Wall 也定义了 n 的非酉因子 d 的概念，即 d 是 n 的因子且 $(d,n/d) > 1$. 如果 n 的非酉因子的和为 n，则称 n 为非酉完全数. 他俩证明：当 $2^p - 1$ 为 Mersenne 素数时 $2^{p+1}(2^p - 1)$ 是非酉完全数. 并且猜想：不存在其它的非酉完全数. Hagis Jr. 证明小于 10^{15} 的奇非酉完全数是不存在的.

[1]H. A. N. Frey, Über unitär perfekte Zahlen, *Elem. Math.*, 33(1978), 95-96, *MR* 81a:10007.

[2]S. W. Graham, Unitary perfect numbers with squarefree odd part, *Fibonacci Quart.*, 27(1989), 4:317-322.

[3]Peter Hagis Jr., Odd nonunitary perfect numbers, *Fibonacci Quart.*, 28(1990), 1:11-15; *MR* 90k:11006.

[4]Steve Ligh and Charles R. Wall, Functions of nonunitary divisors, *Fibonacci Quart.*, 25(1987), 4:333-338.

[5]M. V. Subbarao, Are there an infinity of unitary perfect numbers? *Amer. Math. Monthly*, 77(1970), 389-390.

[6]M. V. Subbarao and D, Suryanarayana, Sums of the divisor and unitary divisor functions, *J. reine angew. Math.*, 302(1978), 1-15; *MR* 80d:10069.

[7]M. V. Subbarao and L. J. Warren, Unitary perfect numbers, *Canad. Math. Bull.*, 9(1966), 147-153; *MR* 33#3994.

[8]M. V. Subbarao, T. J. Cook, R. S. Newberry and J. M. Weber, On unitary perfect numbers, *Delta* 3#1(*Spring* 1972), 22-26.

[9]Charles R. Wall, The fifth unitary perfect number, *Canad. Math. Bull.*, 18(1975), 115-122. See also *Notices Amer. Math. Soc.*, 16(1969), 825.

B4. 互满数、酉互满数

如 $m \neq n$，且 $\sigma(m) = \sigma(n) = m + n$，则称 m,n 为互满数. 已知有上千个互满数存在. 最小的互满数对中，较小的一个是 220，它出现在 Genesis，xxxii，14 中，并且从那时起，互满数就引起了希腊和阿拉伯人的注意. 对于他们的历史，请见 Lee 和 Madachy 的文章.

现在，人们相信存在无穷多对互满数. 事实上，Erdös 猜想，满足 $m < n < x$ 的互满数对的个数 $A(x)$ 至少是 $cx^{1-\epsilon}$. 他改进 Kanold 的一个结果，证明了 $A(x) = o(x)$，并且，用他的方法还能得到 $A(x) \leqslant c\, x/\ln\ln\ln x$，而 Pomerance 则获得了更好的结果：

$$A(x) \leqslant x \exp\{-c(\ln\ln\ln x \ln\ln\ln\ln x)^{1/2}\}.$$

Erdös 猜想，对每一个 k 都有 $A(x) = o(x/(\ln x)^k)$. Pomerance 证明了：

$$A(x) \leqslant x \exp\{-(\ln x)^{1/3}\},$$

因此证实了 Erdös 的猜想. 该结果还推出互满数的倒数和是有限的，这一事实以前是不知道的. Pomerance 也注意到，他的证明可修改一下，给出更强一点的结果：

$$A(x) \ll x \exp\{-c(\ln x \ln\ln x)^{1/3}\}.$$

现在仍不知道是否有 m,n 为一奇一偶或有 $(m,n) = 1$ 的互满数对存在. Bratley 和 McKay 猜想，所有奇互满数对的两个数均能被 3 除尽.

te Riele 发现了若干非常大的互满数对，分别有 32，40，81 和 152 位数. Kaplansky 在 1975 年的"Encyclopedia Brittanica Yearbook"一书的数学条目中提到了 te Riele 的发现. 在这之前知道的互满数对仅有 25 位数.

McClung 研究了酉互满数对 m,n，它满足 $\sigma^*(m) = \sigma^*(n) = m + n$，这里 $\sigma^*(n)$ 表 n 的酉因子(B3)的和. 他用 $\sigma^*(fk) = f\sigma^*(k)$ 定义产生子 (f,k)，这里 f 是有理数，k 和 fk 是整数. 由产生子从已知的一对酉互满数可产生新的酉互满数对. Najar 研究了产生子等

价类的运算.

[1]J. Alanen, O. Ore, and J. G. Stemple, Systematic computations on amicable numbers, *Math. Comp.*, 21(1967), 242-245; *MR* 36#5058.

[2]M. M. Artuhov, On some problems in the theory of amicable numbers (Russian), *Acta Arith.*, 27(1975), 281-291.

[3]W. Borho, On Thabit ibn Kurrah's formula for amicable numbers, *Math. Comp.*, 26(1972), 571-578.

[4]W. Borho, Befreundete Zahlen mit gegebener Primteileranzahl, *Math. Ann.*, 209(1974), 183-193.

[5]W. Borho, Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl, *Math. Nachr.*, 63(1974), 297-301.

[6]W. Borho, Some large primes and amicable numbers, *Math. Comp.*, 36(1981), 303-304.

[7]P. Bratley and J. McKay, More amicable numbers, *Math. Comp.*, 22(1968), 677-678; *MR*37#1299.

[8]P. Bratley, F. Lunnon, and J. McKay, Amicable numbers and their distribution, *Math. Comp.*, 24(1970), 431-432.

[9]B. H. Brown, A new pair of amicable numbers, *Amer. Math. Monthly*, 46(1939), 345.

[10]Patrick Costello, Four new amicable pairs, *Notices Amer. Math. Soc.*, 21(1974), A-483.

[11]Patrick Costello, Amicable pairs of Euler's first form, *Notices Amer. Math. Soc.*, 22(1975), A-440.

[12]P. Erdős, On amicable numbers, *Publ. Math. Debrecen*, 4(1955), 108-111; *MR* 16, 998.

[13]P. Erdős and G. J. Rieger, Ein Nachtrag über befreundete Zahlen, *J. reine angew. Math.*, 273(1975), 220.

[14]E. B. Escott, Amicable numbers, *Scripta Math.*, 12(1946), 61-72; *MR* 8, 135.

[15]M. Garcia, New amicable pairs, *Scripta Math.*, 23(1957), 167-171; *MR* 20 #5158.

[16]A. A. Gioia and A. M. Vaidya, Amicable numbers with oppositc parity, *Amer. Math. Monthly*, 74(1967), 969-973; correction 75 (1968), 386; *MR* 36#3711, 37#1306.

[17]P. Hagis, On relatively prime odd amicable numbers, *Math. Comp.*, 23(1969), 539-543; *MR* 40#85.

[18]P. Hagis, Lower bounds for relatively prime amicable numbers of opposite parity, *ibid*, 24(1970), 963-968.

[19]P, Hagis. Relatively prime amicable numbers of opposite parity, *Math. Mag.*, 43(1970), 14-20.

[20]H. -J. Kanold, Über die Dichten der Mengen der vollkommenen und der befreundeten Zahlen, *Math. Z.*, 61(1954), 180-185; *MR* 16, 337.

[21]H. -J. Kanold, Über befreundete Zahlen I, *Math. Nachr.*, 9(1953), 243-248; II, *idid*, 10(1953), 99-111; *MR* 15, 506.

[22]H. -J. Kanold, Über befreundete Zahlen III, *J. reine angew. Math.*, 234(1969), 207-215; *MR* 39#122.

[23]E. J. Lee, Amicable numbers and the bilinear diophantine equation, *Math. Comp.*, 22(1968), 181-187; *MR* 37#142.

[24]E. J. Lee, On divisibility by nine of the sums of even amicable pairs, *Math. Comp.*, 23(1969), 545-548; *MR* 40#1328.

[25]E. J. Lee and J. S. Madachy, The history and discovery of amicable numbers, part 1, *J. Recreational Math.*, 5(1972), 77-93; part 2, *ibid*, 153-173; part 3, *ibid*, 231-249.

[26]O. W. McClung, *Fibonacci Quart.*, 23(1985), 2:158 — 165; *MR* 87i: 11012a.

[27]Rudolph M. Najar, Operations on generators of unitary amicable pairs, *Fibonacci Quart.*, 27(1989), 2:144—152.

[28]O. Ore, *Number Theory and its History*, McGraw-Hill, New York, 1948, p. 89.

[29]Carl Pomerance, On the distribution of amicable numbers, *J. reine angew. Math.*, 293/294(1977), 217-222; II *ibid*, (1981).

[30]P. Poulet, 43 new couples of amicable numbers, *Scripta Math.*, 14(1948), 77.

[31]H. J. J. te Riele, Four large amicable pairs, *Math. Comp.* ,28(1974), 309-312.

B5. 拟互满数

如果 $\sigma(m)=\sigma(n)=m+n+1, m<n$, 则 Garcia 称数对 (m, n) 为拟互满数. 例如(48,75),(140,195),(1575,1648),(1050,1925)和(2024,2295)都是拟互满数. Rufus Isaacs 注意到 m 和 n 中的每一个都是另一个的真因子的和.

Hagis 和 Lord 已经找到了 $n<10^7$ 的所有 46 对这样的数,它们都具有不同的奇偶性,至今尚未发现有相同奇偶性的 m,n. 如果 m, n 有同样的奇偶性,则 $m>10^{10}$. 如果$(m,n)=1$,那么 mn 至少含有 4 个不同的素因子,并且如果 mn 是奇的,那么 mn 至少有 21 个不同的素因子.

Beck 和 Najar 定义,满足

$$\sigma(m)=\sigma(n)=m+n-1, m<n$$

的 m,n 称为增广互满数. 他们找到了 11 对这样的 m,n,同时还发现,不存在 $n<10^5$ 的增广酉互满数或活泼数 (见 B7).

[1]Walter E. Beck and Rudolph M. Najar, More reduced amicable pairs, *Fibonacci Quart.* ,15(1977),331-332;*Zbl.* 389.10004.

[2]Walter E. Beck and Rudolph M. Najar, Fixed points of certain arithmetic functions, *Fibonacci Quart.* ,15(1977),337-342;*Zbl.* 389.10005.

[3]Peter Hagis and Graham Lord, Quasi-amicable numbers, *Math. Comp.* , 31(1977),608-611;*MR* 55#7902;*Zbl.* 355.10010.

[4]M. Lal and A. Forbes, A note on Chowla's function, *Math. Comp.* , 25(1971),923-925;*MR* 45#6737;*Zbl.* 245.10004.

B6. 整除序列

既然有些数是过剩数,有些数是不足数,那么很自然,人们要问,当作因子和函数的叠代并得到一序列 $\{s^k(n)\}, k=0,1,2,$

…(这里的序列称为整除序列）时将发生什么情况呢？Catalan 和 Dickson 猜想，所有这样的序列都是有界的. 但是，我们现在有直观的推断，几乎对所有偶数 n ，序列将趋于无穷. 曾认为这样最小的偶数 n 为 138，但 D. H. Lehmer 最终证明了，在达到最大值

$$s^{117}(138) = 179931895322 = 2 \times 61 \times 929 \times 1587569$$

之后，该序列将终止在 $s^{177}(138) = 1$ 上. 下一个数是 276，尽管对其存在真正的疑问. 由 Lehmer，接着为 Godwin，Selfridge，Wunderlich 和其他人在作出大量计算后得到

$$s^{469}(276) = 149384846598254844243905695992651412919855640.$$

H. W. Lenstra 已证明，可以构造任意长的单调递增整除序列.

用其它数论函数的叠代将会如何？例如用 $s_e(n)$ 叠代，这里 $s_e(n)$ 表 n 的真指数因子(B16) 的和. 参看 B16 所附 Hagis Jr. 的文章.

[1]Jack Alanen, Empirical study of aliquot series, *Math. Rep.*, 133, Stichting Math. Centrum, Amsterdam, 1972; reviewed *Math. Comp.*, 28(1974), 878-880.

[2]E. Catalan, *Bull. Soc. Math. France*, 16(1887-88), 128-129.

[3]John S. Devitt, Aliquot Sequences, MSc thesis, The Univ. of Calgary, 1976; see *Math. Comp.*, 32(1978), 942-943.

[4]J. S. Devitt, R. K. Guy, and J. L. Selfridge, Third report on aliquot sequences, *Congressus Numeratium* XVIII, Proc. 6th Manitoba Conf. Numerical Math. 1976, 177-204; *MR* 80d:10001.

[5]L. E. Dickson, Theorems and tables on the sum of the divisors of a number, *Quart. J. Math.*, 44(1913), 264-296.

[6]Paul Erdős, On asymptotic properties of aliquot sequences, *Math. Comp.*, 30(1976), 641-645.

[7]Richard K. Guy, Aliquot sequences, in *Number Theory and Algebra*, Academic Press, 1977, 111-118; *MR* 57#223; *Zbl*. 367. 10007.

[8]Richard K. Guy and J. L. Selfridge, Interim report on aliquot series,

Congressus Numerantium V, Proc. Conf. Numerical Math. Winnipeg, 1971, 557-580; *MR* 49#194; *Zbl.* 266.10006.

[9]Richard K. Guy and J. L. Selfridge, Combined report on aliquot sequences, The Univ. of Calgary Math. Res. Report No. 225, May. 1974.

[10]Richard K. Guy and J. L. Selfridge, What drives an aliquot sequence? *Math. Comp.*, 29(1975), 101-107; *MR* 52#5542; *Zbl.* 296.10007. Corrigendum, *ibid*, 34(1980).

[11]Richard K. Guy and M. R. Williams, Aliquot sequences near 10^{12}, *Congressus Numerantium* XII, Proc. 4th Conf. Numerical Math. Winnipeg, 1974, 387-406; *MR* 52#242; *Zbl.* 359.10007.

[12]Richard K. Guy, D. H. Lehmer, J. L. Selfridge, and M. C. Wunderlich, Second report on aliquot sequences, *Congressus Numerantium* IX, Proc. 3rd Conf. Numerical Math. Winnipeg, 1973, 357-368; *MR* 50#4455; *Zbl.* 325.10007.

[13]G. Aaron Paxson, Aliquot sequences (preliminary report), *Amer. Math. Monthly*, 63(1956), 614. See also *Math. Comp.*, 26(1972), 807-809.

[14]P. Poulet, La chasse aux nombres, Fascicule I, Bruxelles, 1929.

[15]H. J. J. te Riele, A note on the Catalan-Dickson conjecture, *Math. Comp.*, 27(1973), 189-192; *MR* 48#3869; *Zbl.* 255.10008.

B7. 整除圈或活泼数

对某个正整数 n，如果存在 t 使 $s^k(n)=s^{k+t}(n)$ 对任何 k 成立，那么 $s^k(n)$ 称为一个整除圈，这样的 n 称为活泼数，最小正整数 t 称为圈的周期. 找到 n 使 $s^k(n)$ 的周期为 1 和 2 是容易的. Poult 找到了两个活泼数使 $s^k(n)$ 的周期分别为 5 和 28. 对 $k\equiv 0,1,2,3,4 \pmod 5$，$s^k(12496)$分别取值为：

$12496=2^4\times 11\times 71$，$14288=2^4\times 19\times 47$，$15472=2^4\times 967$，$14536=2^3\times 23\times 79$，$14264=2^3\times 1783$；

对 $k\equiv 0,1,\cdots,27 \pmod{28}$，$s^k(14316)$取下列值：

14316　19116　31704　47616　83328　177792　295488

629072 589786 294896 358336 418904 366556 274924

275444 243760 376736 381028 285778 152990 122410

97946 48976 45946 22976 22744 19916 17716

时隔 50 多年后，随着高速计算机的出现，Henri Cohen 找到了周期为 4 的 9 个圈. Borho，David 和 Root 又找到了其他的一些圈. 那些周期为 4 的圈的最小元素分别为：

1264460 2115324 2784580 4938136 7169104

18048976 18656380 28158165 46722700 81128632

174277820 209524210 330003580 498215416

人们猜测不存在周期为 3 的圈.

[1] W. Borho, Über die Fixpunkte der k-fach iterierten Teilersummenfunktion, *Mitt. Math. Gesellsch. Hamburg*, 4(1969), 35-38; *MR* 40 # 7189.

[2] H. Cohen, On amicable and sociable numbers, *Math. Comp.*, 24(1970), 423-429; *MR* 42 # 5887.

[3] P. Poulet, Question 4865, *L'Intermediaire des math.*, 25(1918), 100-101.

[4] S. C. Root, in M. Beeler, R. W. Gosper and R. Schroeppel, M. I. T. Artificial Intelligence Memo 239, 1972:02:29.

B8. 酉整除序列

整除序列和整除圈的概念用到仅有酉因子（见 B3）被求和的情形时，则产生了酉整除序列和酉活泼数，与 $\sigma(n)$ 和 $s(n)$ 类似，此时我们用 $\sigma^*(n)$ 和 $s^*(n)$ 表示.

存在无界的酉整除序列吗？值得认真考虑的序列是 6 的奇数倍数序列，因为 6 既是一个酉完全数又是一个普通的完全数. 如果 $3 \| n$，则序列是递增的. 但是，当出现了 3 的高次幂时则递减. 关于是哪种情况占主导地位，现在仍是争论之点. 一旦序列的某项是 $6m$，

m 为奇，那么，除开 3 的奇次幂外，均有 $\sigma^*(6m)$ 是 6 的偶倍数和 $s^*(6m)$ 为 6 的奇倍数吗？

te Riele 对 $n < 10^5$ 讨论了所有的酉整除序列，发现仅有的没有终止或呈周期变化的序列是 89610. 后来的计算表明，此序列在它们第 568 项达到最大值：

$$645856907610421353834$$
$$= 2 \times 3^2 \times 13 \times 19 \times 73 \times 653 \times 3047409443791$$

且在它的第 1129 项结束.

只有素因子的期望值很大时，才能预测序列的典型特性，但素因子大到 $\ln \ln n$ 时，序列又已远远超出了计算机的范围. 在已考察的 10^{12} 附近的 80 个序列中，全都为终止或趋向周期化. 其中一个序列超过 10^{23}.

酉互满数和酉活泼数可能比其普通数出现得更经常一些. Lal, Tiller 和 Summers 找到了周期为 1,2,3,4,5,6,14,25,39 和 65 的圈，酉互满对的例子是(56430,64530)和(1080150,1291050)，而(30,42,54)是周期为 3 的圈，(1482,1878,1890,2142,2178)是周期为 5 的圈.

Erdős 一直想找到一个数论函数，其叠代可能为有界. 他定义 $W(n) = n\sum 1/p_i^{a_i}$，其中 $n = \prod p_i^{a_i}$，且 $W^k(n) = W(W^{k-1}(n))$. 注意到 $(W(n), n) = 1$，那么能证明 $W^k(n)$ $(k = 1,2,\cdots)$ 是有界的吗？又 $|\{W(n) : 1 \leqslant n \leqslant x\}| = o(x)$ 成立吗？

如果对所有的 $m < n$ 使得 $m + f(m) \leqslant n$，则 Erdős 和 Selfridge 称 n 为数论函数 $f(n)$ 的闸. Euler 的 φ 函数(见 $B36$) 和 $\sigma(m)$ 增加得太快以致于没有闸. 但是，另一方面，m 的不同素因子的个数 $\omega(m)$ 有无穷多个闸吗？现已知 2,3,4,5,6,8,9,10,12,14,17,18,20,24,26,28,30,… 都是 $\omega(m)$ 的闸. 如果 $\Omega(m)$ 是 m 的素因子的个数(素因子不是必须互异)，那么 $\Omega(m)$ 有无穷多个闸吗？Selfridge 注意到，99840 是 $\Omega(m) < 10^5$ 的最大的闸. m 的因子个数 $d(m)$ 没有闸，因为 $\max\{d(n-1)+n-1, d(n-2)+n-2\} \geqslant$

$n+2$，而

$$\max_{m<n}(m+d(m))=n+2$$

有无穷多组解吗？这是非常令人怀疑的．其一解为 $n=24$，下一个较大的解大概又超出了计算机的范围．

[1]Paul Erdös, A melange of simply posed conjectures with frustratingly elusive solutions, *Math. Mag.*, 52(1979)67-70.

[2]P. Erdös, Problems and results in number theory and graph theory, *Congressus Numerantium XXVII*, Proc. 9th Manitoba Conf. Numerical Math. Comput., 1979, 3-21.

[3]Richard K. Guy and Marvin C. Wunderlich, Computing unitary aliquot sequences—a preliminary report, *Congressus Numerantium XXVII*, Porc. 9th Manitoba Cont. Numerical Math. Comput., 1979, 257-270.

[4]P. Hagis, Unitary amicable numbers, *Math. Comp.*, 25(1971), 915-918; *MR* 45#8599; *Zbl.* 232.10004.

[5]Peter Hagis, Unitary hyperperfect numbers, *Math. Comp.*, 36(1981), 299-301.

[6]M. Lal, G. Tiller and T. Summers, Unitary sociable numbers, *Congressus Numerantium* VII, Proc. 2nd Conf. Numerical Math. Winnipeg, 1972, 211-216; *MR* 50#4471; *Zbl.* 309.10005.

[7]H. J. J. te Riele, *Unitary Aliquot Sequences*, *MR* 139/72, Mathematisch Centrum, Amsterdam, 1972; reviewed *Math. Comp.*, 32(1978), 944-945; *Zbl.* 251.10008.

[8]H. J. J. te Riele, *Further Results on Unitary Aliquot Sequences*, NW2/73, Mathematisch Centrum, Amsterdam, 1973; reviewed *Math. Comp.*, 32(1978), 945.

[9]H. J. J. te Riele, *A Theoretical and Computational Study of Generalized Aliquot Sequences*, MCT74, Mathematisch Centrum, Amsterdam, 1976; reviewed *Math. Comp.*, 32(1978), 945-946; *MR* 58#27716.

[10]C. R. Wall, Topics related to the sum of unitary divisors of an integer, PhD thesis, Univ. of Tennessee, 1970.

B9. 超完全数

Suryanarayana 用 $\sigma^2(n) = 2n$ 定义了超完全数，即 n 满足 $\sigma(\sigma(n)) = 2n$. 他和 Kanold 证明，偶超完全数恰是 2^{p-1}，其中 p 满足 $2^p - 1$ 为 Mensenne 素数. 存在奇超完全数吗？如存在，则 Kanold 证明了，它们是完全平方数. Dandapat 等人证明了，n 或 $\sigma(n)$ 至少可被三个不同素数整除.

更一般地，Bode 称满足 $\sigma^m(n) = 2n$ 的 n 为 m 重完全数，且证明了对 $m \geqslant 3$，不存在偶的 m 重完全数. 他还证明了，对于 $m = 2$，不存在 $< 10^{10}$ 的奇超完全数. Hunsucker 和 Pomerance 已改进这个上界到 7×10^{24}，并且他们还得到了关于 n 为超完全数时，n 和 $\sigma(n)$ 的不同素因子的个数的结果.

如果 $\sigma^2(n) = 2n + 1$，此时它将与早先把 n 称为拟完全数的术语相一致. Mersenne 素数便是这样的数，还有其他的拟超完全数吗？存在"几乎超完全数"使 $\sigma^2(n) = 2n - 1$ 吗？

Erdös 问，当 $k \to \infty$ 时，$(\sigma^k(n))^{1/k}$ 是否有极限？他猜想，对每一个 $n > 1$，它为无穷.

Schinzel 问，当 $n \to \infty$ 时，对每个 k，是否有

$$\liminf \sigma^k(n)/n < \infty ?$$

他观察到，对 $k = 2$，由 Rényi 的很深的定理，上式将成立. Makowski 和 Schinzel 给出 $k = 2$ 时上述极限为 1 的初等证明.

[1]Dieter Bode, Über eine Verallgemeinerung der Vollkommenen Zahlen, Dissertation, Braunschweig, 1971.

[2]P. Erdös, Some remarks on the iterates of the φ and σ functions, *Colloq. Math.*, 17(1967), 195-202.

[3]J. L. Hunsucker and C. Pomerance, There are no odd superperfect numbers less than 7×10^{24}, *Indian J. Math.*, 17(1975), 107-120.

[4]H.-J. Kanold, Über "Super perfect numbers," *Elem. Math.*, 24(1969), 61-62; *MR* 39#5463.

[5]Graham Lord, Even perfect and superperfect numbers, *Elem. Math.*, 30(1975), 87-88.

[6]A. Makowski and A. Schinzel, On the functions $\varphi(n)$ and $\sigma(n)$, *Colloq. Math.*, 13(1964-65), 95-99.

[7]A. Schinzel, Ungelöste Probleme Nr. 30, *Elem. Math.*, 14(1959), 60-61.

[8] D. Suryanarayana, Super perfect numbers, *Elem. Math.*, 24(1969), 16-17; *MR* 39#5706.

[9]D. Suryanarayana, There is no odd superperfect number of the form p^{2a}, *Elem. Math.*, 28(1973), 148-150.

B10. 不可摸数

Erdös 已证明，存在无穷多个 n 使 $s(x)=n$ 没有解. Alanen 称这样的 n 为不可摸数(untouchable). 事实上，Erdös 证明了不可摸数具有正的小密率. 下面是一些<1000 的不可摸数：

2 5 52 88 96 120 124 146 162 178 188 206 210 216 238 246
248 262 268 276 288 290 292 304 307 322 324 326 336 342 372 406
408 426 430 448 472 474 498 516 518 520 530 540 552 556 562 576
584 612 624 626 628 658 668 670 714 718 726 732 738 748 750 756
766 768 782 784 792 802 804 818 836 848 852 872 892 894 896 898
902 916 926 936 964 966 976 982 996

从 Goldbach 猜想(C1)似乎成立的观点来看，5 为唯一的奇不可摸数大概是可能的，因为如果 $2n+1=p+q+1$，p,q 为不同的素数，则 $s(pq)=2n+1$. 这能独立地被证明吗？存在任意长的连续偶不可摸数序列吗？不可摸数的区间间隔能是多大？

[1]P. Erdös, Über die Zahlen der Form $\sigma(n)-n$ und $n-\varphi(n)$, *Elem. Math.*, 28(1973), 83-86.

[2] Paul Erdös, Some unconventional problems in number theory, *Astérisque*, 61(1979), 73-82; *Zbl.* 399. 10001; *MR* 81h: 10001.

B11. $m\sigma_k(m)=n\sigma_k(n)$的解

Leo Moser 已经注意到，$n\varphi(n)$ 唯一地确定 n 而 $n\sigma(n)$ 则不能（$\varphi(n)$ 是 Euler 函数，见 B27）. 例如，$m\sigma(m)=n\sigma(n)$ 对于 $m=12$，$n=14$ 成立. 现在 $\sigma(n)$ 的积性保证了 $m\sigma(m)=n\sigma(n)$ 的解有无穷多个，例如 $m=12q$，$n=14q$，其中 $(q,42)=1$. 因此，Moser 问是否有无穷多组原始解（例如 $m=12$，$n=14$ 是原始解）. 在这个意义上，对任意的 $m^*=m/d$，$n^*=n/d$，$d>1$，(m^*,n^*) 不是解. 我们给出的例子是解 $m=2^{p-1}(2^q-1)$，$n=2^{q-1}(2^p-1)$ 中最小的一组，其中 2^p-1，2^q-1 是不同的 Mesenne 素数，因而，这些解仅知道有限个. 另一类解是：$m=2^7\times3^2\times5^2\times(2^p-1)$，$n=2^{p-1}\times5^3\times17\times31$，其中 2^p-1 是除开 3 或 31 外的 Mesenne 素数；$p=5$ 在剔除公因子 31 后也给出原始解. 还存在其他的解，如 $m=2^4\times3\times5^3\times7$，$n=2^{11}\times5^2$ 和 $m=2^9\times5$，$n=2^3\times11\times31$. 一个满足 $(m,n)=1$ 的例子为 $m=2^5\times5$，$n=3^3\times7$.

Erdös 观察到，如 n 是无平方因子数，那么形如 $n\sigma(n)$ 的整数是两两不同的. 他还能证明，$m\sigma(m)=n\sigma(n)$ 满足 $m<n<x$ 的解的个数是 $cx+o(x)$. 存在三个不同数 l,m,n 使 $l\sigma(l)=m\sigma(m)=n\sigma(n)$ 吗？方程 $\sigma(a)/a=\sigma(b)/b$ 存在无穷多个原始解吗？如不限制解为原始的，Erdös 证明了满足 $a<b<x$ 的解的个数为 $cx+o(x)$. 如限制 $(a,b)=1$，至今尚不知道是否存在解.

Erdös 认为，对于任意的 $\varepsilon>0$，方程 $x\sigma(x)=n$ 解的个数小于 $n^{\varepsilon/\ln\ln n}$，并且他说解的个数可能小于 $(\ln n)^c$.

用 $\sigma_k(n)$ 代替 $\sigma(n)$ 可以提出一些类似的问题，其中 $\sigma_k(n)$ 是 n 的因子的 k 次幂的和，例如，存在不同数 m,n 使 $m\sigma_2(m)=n\sigma_2(n)$ 吗？对于 $k=0$ 的情形，我们得到 $md(m)=nd(n)$ 有解 $(m,n)=(18,27)$，$(24,32)$，$(56,64)$ 和 $(192,224)$，而且最后一对再添上 168，给出三个不同的数 l,m,n 使 $ld(l)=md(m)=nd(n)$ 成立. 此外，$md(m)=nd(n)$ 存在无穷多组原始解 (m,n)，例如：

$$m=2^{q^t-1}p,\quad n=2^{p^u\cdot 2^{tu}-1}q,$$

其中 p 和 $q = u + p \cdot 2^m$ 是素数. 许多另外的解能被构造出来，例如 $(2^{70}, 2^{63} \times 71)$，$(3^{19}, 3^{17} \times 5)$ 和 $(5^{51}, 5^{49} \times 13)$.

柯召和孙琦不限制为原始解证明了 $a(d(n))^s = b(\varphi(n))^t$，$a(\sigma(n))^t = b(\varphi(n))^s (s \neq t)$，$a(\sigma(n))^s = b(d(n))^t$ 以及 $a(\sigma(n))^t = bn(d(n))^s$ 均仅有有限个解，这里 a,b,s 和 t 均是给定的正整数. 但 $a(\sigma(n))^s = b(\varphi(n))^s$ 是否仅有有限个解？

[1]P. Erdős, Remarks on number theory II: some problems on the σ function-, *Acta Arith.*, 5(1959), 171-177; *MR* 21#6348.

[2]柯召(C. Ko)，孙琦，论一类型积性数论函数方程，四川大学学报(自然科学版)，2(1965)，1－10.

B12. $\sigma_k(n) = \sigma_k(n+l)$ 的解

Sierpinski 问是否存在无穷多个 n 使 $\sigma(n) = \sigma(n+1)$？Hunsucker 等人扩充了 Makowski 以及 Mientka 和 Vogt 的表，并且已经找到 $<10^7$ 的113组解：

14, 206, 957, 1334, 1364, 1634, 2685, 2974, 4364, …

他们还获得了与方程 $\sigma(n) = \sigma(n+l)$ 有关的统计表. Mientka 和 Vogt 问，对怎样的 l(如果有)，$\sigma(n) = \sigma(n+l)$ 有无穷多组解？如果 l 是阶乘，他们找到了许多组解. 但 $l = 15$ 和 $l = 19$ 时仅有两组解. 他们又问，对每一个 l 和 m，是否存在 n 使 $\sigma(n) + m = \sigma(n+l)$ 成立？

对于 $\sigma_k(n)$(见 B11)，人们可提相应的问题. $\sigma_2(n) = \sigma_2(n+1)$ 仅有解是 $n = 6$，因为对于 $n > 7$ 有 $\sigma_2(2n) > \sigma_2(2n+1)$. 注意到 $\sigma_2(24) = \sigma_2(26)$；Erdős 怀疑 $\sigma_2(n) = \sigma_2(n+2)$ 有无穷多组解，并且他认为，$\sigma_3(n) = \sigma_3(n+2)$ 完全没有解.

[1]Richard K. Guy and Daniel Shanks, A constructed solution of $\sigma(n) = \sigma(n+1)$, *Fibonacci Quart.*, 12(1974), 299; *MR* 50#219; *Zbl.* 287.10004.

[2]John L. Hunsucker, Jack Nebb, and Robert E. Stearns, Computational results con-cerning some equations involving $\sigma(n)$, *Math. Student*, 41(1973), 285-289.

[3] A. Makowski, On some equations involving functions $\varphi(n)$ and $\sigma(n)$, *Amer. Math. Monthly*, 67(1960), 668-70 correction, *ibid.* 68(1971), 650.

[4]W. E. Mientka and R. L. Vogt, Computational results relating to problems concerning $\sigma(n)$, *Mat. Vesnik*, 7(1970), 35-36.

B13. 一个无理数问题

$\sum_{n=1}^{\infty}(\sigma_k(n)/n!)$ 是无理数吗?已知对 $k=1,2$,它是如此.

[1]P. Erdős and M. Kac, Problem 4518, *Amer. Math. Monthly*, 60(1953), 47. Solution, R. Breusch, 61(1954), 264-265.

B14. $\sigma(q)+\sigma(r)=\sigma(q+r)$的解

Max Rumney(*Eureka*, 26(1963), 12)问是否方程 $\sigma(q)+\sigma(r)=\sigma(q+r)$ 有无穷多组原始解?这里的原始解与B11 中的定义类似. 如果$q+r$是素数,则$\sigma(q)+\sigma(r)=\sigma(q+r)$ 仅有的解是$(q,r)=(1,2)$. 如果 $q+r=p^2$,其中 p 是素数,则由 $\sigma(q)+\sigma(r)=\sigma(q+r)$ 推出 q,r 之一是素数,且如q 是素数,则$r=2^n k^2$,其中 $n\geq 1$, $2\nmid k$. 如果 $k=1$,且 $p=2^n-1$ 是 Mersenne 素数,$q=p^2-2^n$ 是素数,则方程有解. 例如 $n=2,3,5,7,13$ 和 19 是这样的. 对 $k=3$,没有解,并且对 $k=5$ 也没有 $n<189$ 的解. 对 $k=7$,$n=1$ 和 3 时,有解$(q,r,q+r)=(5231,2\times 7^2,73^2)$ 和$(213977,2^3\times 7^2,463^2)$. 其他的解是:$(k,n)=(11,1),(11,3),(19,5),(25,1),(25,9),(49,9),(53,1),(97,5),(107,5),(131,5),(137,1),(149,5),(257,5),(277,1),(313,3)$ 和$(421,3)$. 满足$q+r=p^3$ 且 p 是素数的解为:$\sigma(2)+\sigma(6)=\sigma(8)$ 和

$$\sigma(11638678)+\sigma(2^2\times 13\times 1123)=\sigma(227^3).$$

Erdös 问，$q+r<x$ 时，$\sigma(q)+\sigma(r)=\sigma(q+r)$ 有多少组解（不一定是原始的）；它是 $cx+o(x)$ 或具有更高的阶吗？如果 $s_1<s_2<\cdots$ 这里 s_i 使 $\sigma(s_i)=\sigma(q)+\sigma(s_i-q)$，$q<s_i$ 有解，那么序列 $\{s_i\}$ 的密率是什么？

[1]M. Sogunamma, PhD thesis, Sri Venkataswara Univ. 1969.

B15. **幂数问题**

Erdös 和 Szekeres 研究了这样一些数 n：如果素数 p 除尽 n，那么 p^i 也除尽 n，其中 $i>1$ 是给定的. Golomb 定义这些数为幂数，且得出有无穷多对相邻的幂数. 他猜想，6不能表为两个幂数的差，以及存在无穷多个不能表为两个幂数差的数. 另一方面，Makowski 已证明，每一素数 $\equiv 1 \pmod 8$ 均是两互素幂数的差. Sentance 已发现，除开 $(5^2, 3^3)$ 外，还有无穷多对这样的连续奇幂数. 事实上，Golomb 猜想是不成立的，例如肖戎给出 $6=5^4\cdot7^3-463^2$. 对一般情形，Mollin 和 Walsh，孙琦和袁平之，曹珍富用丢番图方程 $x^2-dy^2=c$ 的解，构造性地证明了：任一数均可表为两互素幂数之差，且表法无穷. 并且这两个幂数还可以满足一些条件，例如前一个是平方数，或两个均是非平方幂数.

Erdös 用 $u_1^{(k)}<u_2^{(k)}<\cdots$ 表示那些素因子的指数 $\geqslant k$ 的幂数. 他问方程 $u_{i+1}^{(2)}-u_i^{(2)}=1$ 是否有无穷多组不为完全平方数的解？对这个问题，肖戎给出了肯定地回答. Erdös 问存在常数 c，使 $u_{i+1}{}^{(2)}-u_i{}^{(2}=1$ 在 $u_i{}^{(2)}<x$ 时的解数小于 $(\ln x)^c$ 吗？$u_{i+1}{}^{(3)}-u_i{}^{(3)}=1$ 没有解吗？$u_{i+2}^{(2)}-u_{i+1}^{(2)}=1=u_{i+1}^{(2)}-u_i^{(2)}$ 没有联立解吗？使 $u_{i_1}^{(2)},\cdots,u_{i_r}^{(2)}$ 以等差数列形式存在的最大的 r 是多少？Erdös 猜想，(1)存在无穷多个三元组 $u_{i_1}^{(3)}, u_{i_2}{}^{(3)}, u_{i_3}{}^{(3)}$ 成等差数列，不存在四元组 $u_{i_1}{}^{(3)},\cdots,u_{i_4}{}^{(3)}$ 成等差数列，且不存在三元组 $u_{i_1}{}^{(4)}, u_{i_2}{}^{(4)}, u_{i_3}{}^{(4)}$ 成等差数列；(2)$u_i^{(3)}+u_j^{(3)}=u_k^{(3)}$ 有无穷多组解，但是，$u_i^{(4)}+u_j^{(4)}=u_k^{(4)}$ 最多只有有限组解. 更一般地，$k-2$ 个 $u_i^{(k)}$ 的和至多有限次为 $u_i^{(k)}$；(3) 每

一充分大的整数是 3 个 $u_i^{(2)}$ 的和,他要求得到那些不是 3 个 $u_i^{(2)}$ 之和的整数表.

[1]曹珍富(Zhen Fu Cao),丢番图方程引论,第五章,哈尔滨工业大学出版社,1989.

[2] P. Erdös, Problems and results on consecutive integers, *Eureka*, 38(1975-76),3-8.

[3]P. Erdös and G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung undüber ein verwandtes zahlentheoretisches Problem, *Acta Litt. Sci. Szeged*,7(1934),95-102;*Zbl.* 10,294.

[4] S. W. Golomb, Powerful numbers, *Amer. Math. Monthly*,77(1970), 848-852;*MR* 42#1780.

[5]Andrzej Makowski, On a problem of Golomb on powerful numbers, *Amer. Math. Monthly*,79(1972),761.

[6]R. A. Mollin and P. G. Walsh, Proper differences of nonsquare powerful numbers, *C. R. Math. Rep. Acad. Sci. Canada*, 10(1988),2:71－76.

[7]W. A. Sentance, Occurences of consecutive odd powerful numbers, *Amer. Math. Monthly*,88(1981),272-274.

[8]孙琦(Q. Sun),袁平之,关于一些幂数问题,四川大学学报(自然科学版),26(1989),3:277－282.

[9]肖戎 (R. Xiao),关于幂数的几个问题,数学研究与评论,3(1987),408－410.

B16. e-完全数

如果 $n = p_1^{a_1}\cdots p_r^{a_r}$,且 $d|n$ 和 $d = p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}$,其中 $b_j|a_j(1 \leqslant j \leqslant r)$,那么 ,Straus 和 Subbarao 称 d 是 n 的指数因子(e- 因子). 如果 $\sigma_e(n) = 2n$,其中 $\sigma_e(n)$ 是 n 的指数因子之和,则他们称这样的 n 是 e- 完全数. 一些 e- 完全数的例子是:

$2^2 \times 3^2$, $2^2 \times 3^3 \times 5^2$, $2^3 \times 3^2 \times 5^2$, $2^4 \times 3^2 \times 11^2$, $2^4 \times 3^3 \times 5^2 \times 11^2$, $2^6 \times 3^2 \times 7^2 \times 13^2$, $2^6 \times 3^3 \times 5^2 \times 7^2 \times 13^2$, $2^7 \times 3^3 \times 5^2 \times 7^2 \times 13^2$, $2^8 \times 3^2 \times 5^2 \times 7^2 \times 139^2$

和

$2^{19}\times3^2\times5^2\times7^2\times11^2\times13^2\times19^2\times37^2\times79^2\times109^2\times157^2\times313^2$.

设 m 是无平方因子，则 $\sigma_e(m) = m$. 因此，如果 n 是 e- 完全数，m 为无平方因子数且 $(m,n) = 1$，则 mn 是 e- 完全数. 因此，下面只考虑幂数(B15) 的 e- 完全数.

Straus 和 Subbarao 证明：不存在奇 e- 完全数. 事实上，对任意整数 $k > 1$，不存在满足 $\sigma_e(n) = kn$ 的奇数 n. 他们还证明了，对于每一个 r，具有 r 个素因子的幂数 e- 完全数的个数是有限的.

Hagis Jr. 证明了：e- 完全数的密率是 0.0087. 他还得到与指数因子有关的其它一些结果.

存在不能被 3 整除的 e- 完全数吗?

Straus 和 Subbarao 猜想，仅有有限个 e-完全数不能被给定的素数 p 整除.

[1]Peter Hagis Jr. ,Some results concerning exponential divisors, *Internat. J. Math. Sci.* , 11(1988),2:343—349.

[2]E. G. Straus and M. V. Subbarao,On exponential divisors, *Duke Math. J.* 41(1974),465-471;*MR* 50#2053.

[3]M. V. Subbarao, On some arithmetic convolutions, in *The Theory of Arithmetic Functions*, Springer-Verlag, New York, 1972.

[4]M. V. Subbarao and D. Suryanarayana, Exponentially perfect and unitary perfect numbers, *Notices Amer. Math. Soc.* ,18(1971),798.

B17. $d(n)=d(n+1)$的解

存在无穷多个 n 使 $d(n) = d(n+1)$ 吗?例如，$n = 2,14,21,26,33,34,38,44,57,75,85,86,93,94,98,104,116,118,122,133,135,141,142,145,147,\cdots$ 时，$d(n) = d(n+1)$ 都成立. 在这些例中，有许多是从恰有两个不同素数乘积的连续数对中产生的. 人们猜想使连续的三个数 $n, n+1, n+2$ 都恰是两个不同素数乘积的 n 有无穷多个. 例如，$n = 33,85,93,141,201,213,217,301,393$,

445,633,697,921,… 显然不可能有四个这样的连续数，因为其中必然有一个被2^2整除. 但我们有一个直观的猜想：有无穷多四个连续数，它们都恰含两个不同素因子. 此外，具有相同因子个数的连续数的长序列是存在的，如：

$$d(242) = d(243) = d(244) = d(245) = 6$$

和

$$d(40311) = d(40312) = d(40313) = d(40314) = d(40315) = 8$$

那么，这样的序列能有多长呢？

[1]P. Erdős and L. Mirsky, The distribution of values of the divisor function $d(n)$, *Proc. London Math. Soc.*, (3)2(1952), 257-271.

[2]M. Nair and P. Shiu, On some results of Erdős and Mirsky, *J. London Math. Soc.*, (2)22(1980), 197-203; and see *ibid.* 17(1978)228-230.

[3]A. Schinzel, Sur un problème concernant le nombre de diviseurs d'un nombre naturel, *Bull. Acad. Polon. Sci. Ser. sci. math. astr. phys.*, 6(1958), 165-167.

[4]A. Schinzel and W. Sierpinski, Sur certaines hypothéses concernant les nombres premiers, *Acta Arith.*, 4(1958), 185-208.

[5]W. Sierpinski, Sur une question concernant le nombre de diviseurs premiers d'un nombre naturel, *Colloq. Math.*, 6(1958), 209-210.

B18. 相同素因子问题

Motzkin 和 Straus 提出求所有的数对 m,n 使 m 和 $n+1$，以及 n 和 $m+1$ 分别有相同的不同素因子的集合. 人们一直认为这样的数对必定形如 $m = 2^k + 1, n = m^2 - 1 (k = 0,1,2,\cdots)$，直到 J. H. Conway 发现，如果 $m = 5 \times 7, n + 1 = 5^4 \times 7$，则 $n = 2 \times 3^7, m + 1 = 2^2 \times 3^2$，才改变了这个看法. 那么还有其他的吗？

类似地，Erdős 问，除开 $m = 2^k - 2, n = 2^k(2^k - 2)$ 外，是否还有其他的数 $m, n (m < n)$ 使 m 和 n，以及 $m+1$ 和 $n+1$ 分别具有同样的素因子？Makowski 找到 $m = 3 \times 5^2, n = 3^5 \times 5$，且 $m+1$

$= 2^2 \times 19, n + 1 = 2^6 \times 19$. 类似的问题还可以提出很多,但有应用背景的不多.

Pomerance 猜想:不存在奇数 $n > 1$ 使 n 和 $\sigma(n)$ 有同样的素因子. 这还没有证明.

[1] A. Makowski, On a problem of Erdös, *Enseignement Math.*, (2) 14 (1968), 193.

B19. **形如 $k \times 2^m + 1$ 的素数**

一些人研究了 Cullen 数 $n \times 2^n + 1$,发现除了 $n = 141$ 外,对 $2 \leqslant n \leqslant 1000$, 它均是合数. 那么 Cullen 数中到底有多少素数?有限的还是无限的?很容易证明,有无限多个 Cullen 数是合数,例如当 $n \equiv 1 (\bmod 6)$ 时 Cullen 数均被 3 整除. 根据 Fermat 小定理,当 p 是奇素数时, $(p-1)2^{p-1}+1$ 和 $(p-2) \cdot 2^{p-2}+1$ 均能被 p 除尽. 所以 Cullen 数非常可能是合数.

Riesel 得到,相应的数 $n \times 2^n - 1$ 在 $n \leqslant 110$ 时仅当 $n = 2, 3, 6, 30, 75$ 和 81 时是素数.

设正奇数 k 使 $k \cdot 2^n + 1$ 对于某些正整数 n 为素数, $N(x)$ 是这些正奇数 $k \leqslant x$ 的个数, Sierpinski 用覆盖同余(见 F12)证明, $N(x)$ 随 x 趋向无穷,例如,如果

$k \equiv 1 (\bmod 641 \times (2^{32} - 1))$ 和 $k \equiv -1 (\bmod 6700417)$,

那么,序列 $k \cdot 2^n + 1 (n = 0, 1, 2, \cdots)$ 的每一个数均至少能被素数 3, 5, 17, 257, 641, 65537 和 6700417 中的一个整除. 他注意到,对于 k 的特定的其他值,均有 3, 5, 7, 13, 17, 241 中的一个整除 $k \cdot 2^n + 1$.

Erdös 和 Odlyzko 已证明:

$$\left(\frac{1}{2} - c_1\right)x \geqslant N(x) \geqslant c_2 x.$$

使 $k \cdot 2^n + 1$ 对所有 n 均为合数的最小 k 是什么? Selfridge 发

现,3,5,7,13,19,37,73总能整除 $78557\times 2^n+1$. 他又注意到,对 $k<383$,存在形如 $k\cdot 2^n+1$ 的素数,且 $383\times 2^n+1$ 对所有 $n<2313$ 为合数. N. S. Mendelsohn 和 B. Wolk 改进这一结果到 $n\leqslant 4017$,但是,最近,Hugh Williams 找到了素数 $383\times 2^{6393}+1$.

似乎最小 k 值的确定能用计算机来完成. Baillie, Cormack 和 Williams 作了大范围的计算,发现了若干个形如 $k\cdot 2^n+1$ 的素数,其中包括

$$k=2897,6313,7493,7957,8543,9323$$

和

$$n=9715,4606,5249,5064,5793,3013,$$

但是仍剩下118个小于78557的未作考察. 这些数中的头8个是

$$k=3061,4847,5297,5359,5897,7013,7651\text{和}8423.$$

对于这些 k, 已知各自当

$$n\leqslant 16000,8102,8070,8109,8170,8105,8080\text{和}8000$$

时没有素数存在.

[1]G. V. Cormack and H. C. Williams, Some very large primes of the form $k\cdot 2^n+1$, *Math. Comp.*, 35(1980), 1419-1421; *MR* 81i:10011.

[2]P. Erdös and A. M. Odlyzko, On the density of odd integers of the form $(p-1)2^{-n}$ and related questions, *J. Number Theory*, 11(1979), 257-263.

[3] J. L. Selfridge, Solution to problem 4995, *Amer. Math. Monthly*, 70(1963), 101.

[4]W. Sierpinski, Sur un probléme concernant les nombres $k\cdot 2^n+1$, *Elem. Math.* 15(1960), 73-74; *MR* 22#7983; corrigendum, *ibid*. 17(1962), 85.

[5]W. Sierpinski, 250 *Problems in Elementary Number Theory*, Elsevier, New York, 1970, 10. 64.

B20. 将 n!分解成某些因子乘积

Straus, Erdös 和 Selfridge 提出,试将 n!表为 n 个因子的乘积,且要求最小的一个因子 l 尽可能大. 例如,对 $n=56$,有 $l=15$,

因为

$$56!=15\times16^3\times17^3\times18^8\times19^2\times20^{12}\times21^9\times22^5\times23^2\times26^4\times29\times31\times37\times41\times43\times47\times53.$$

Selfridge 有两个猜想：a) 除开 $n=56$，均有 $l\geqslant[2n/7]$；b) 对 $n\geqslant300000$，有 $l\geqslant n/3$（如果此为真，那么，300000能被更小的代替吗?）并且 Erdös，Selfridge 和 Straus 已证明，对于 $n>n_0=n_0(\varepsilon)$，有 $l>n/(e+\varepsilon)$. 从 Stirling 公式看，显然它是可能达到的最好结果. Straus 仅借助变化2的幂的位置已证明 $l\geqslant3n/16$. 显然，l 是 n 的单调函数（当然，尽管不是严格地）. 另一方面，l 不取遍所有整数值，对 $n=124,125$，l 分别是35，37. Erdös 问，l 值中的间隔能是多大呢?对任意大的范围，l 能是常数吗?

Alladi 和 Grinstead 表 $n!$ 为素数幂的乘积，每一个均如 $n^{\delta(n)}$ 一样大，且设 $\alpha(n)=\max\delta(n)$，他们证明了 $\lim\limits_{n\to\infty}\alpha(n)=e^{c-1}=\alpha$，其中

$$c=\sum_{k=2}^{\infty}\frac{1}{k}\ln\frac{k}{k-1},$$

因此，$\alpha=0.809394020534\cdots$.

假定 $n!=a_1!a_2!\cdots a_r!$，$r\geqslant2$，$a_1\geqslant a_2\geqslant\cdots\geqslant a_r\geqslant2$，一个平凡的例子是 $a_1=a_2!\cdots a_r!-1$，$n=a_2!\cdots a_r!$. Dean Hickerson 注意到，当 $n\leqslant410$ 时，仅有的非平凡例子是 $9!=7!3!3!2!$，$10!=7!6!=7!5!3!$ 和 $16!=14!5!2!$，他问还有其他的例子吗?

Erdös 注意到，如 $p(n)$ 是 n 的最大素因子，且如果已知 $p(n(n+1))/\ln n$ 随 n 趋于无穷，那么仅有有限个非平凡例子吗?

Erdös 和 Graham 已经研究了方程 $y^2=a_1!a_2!\cdots a_r!$，他们定义集合 F_k 是整数 m 的集合，这里 $m=a_1>a_2>\cdots>a_r(r\leqslant k)$ 对于某些 y 满足方程. D_k 为 F_k-F_{k-1}，则可得到各种结果，例如，对于几乎所有素数 p，$13p$ 不属于 F_5，且 D_6 的最小元素为 527. 如果 $D_4(n)$ 是 D_4 中的元素 $\leqslant n$ 的个数，他们说：不知道 $D_4(n)$ 增长的阶为何?他们猜想，$D_6(n)>cn$，但不能证明它.

[1]K. Alladi and C. Grinstead, On the decomposition of $n!$ into prime powers, *J. Number Theory*, 9(1977), 452-458.

[2] E. Ecklund and R. Eggleton, Prime factors of consecutive integers, *Amer. Math. Monthly*, 79(1972), 1082-1089.

[3]E. Ecklund, R. Eggleton, P. Erdős and J. L. Selfridge, On the prime factorization of binomial coeffcients, *J. Austral Math. Soc. Ser.* A, 26 (1978), 257-269; *MR* 80e: 10009.

[4] P. Erdős, Some problems in number theory, *Computers in Number Theory*, Academic Press, London and New York, 1971, 405-414.

[5]P. Erdős, Problems and results on number theoretic properties of consecutive integers and related questions, *Congressus Numerantium XVI* Proc. 5th Manitoba Conf. Numer. Math., 1975, 25-44.

[6]P. Erdős and R. L. Graham, On products of factorials, *Bull. Inst. Math. Acad. Sinica, Taiwan*, 4(1976)337-355.

B21. $[1,n]$的某些最大子集

考虑 $[1,n]$ 中没有一个元素能除尽其他任何两个元素的子集. 假设 $f(n)$ 是这样子集中的最大子集的元素个数,Erdős 问 $f(n)$ 能有多大?如取$[m+1,3m+2]$,显然,$f(n)$ 为$\langle 2n/3\rangle$. D. J. Kleitman 证明,如取$[11,30]$,且$[11,30]$中不含有18,24,30,但它允许包含6,8,9和10,则 $f(29)=21$. 但是,该例子似乎不一般化,事实上,Lebensold 已证明,如 n 很大,则

$$0.6725n \leqslant f(n) \leqslant 0.6736n.$$

相应地,在不超过 n 的数中,寻找一最大集合,该集合中没有一个元素能是其他二元素的倍数. 上述 Kleitman 的例子也能用于这个问题. 更一般地,Erdős 问,不超过 n 且没有一个数能被其他 k 个数除尽的数的最大个数是多少($k>2$)?对 $k=1$,答案是$\langle n/2\rangle$.

Bateman 问 $31=(2^5-1)/(2-1)=(5^3-1)/(5-1)$ 是否是仅有的可用多于一种方式表达为$(p^r-1)/(p^d-1)$ 的素数,其中 p 是素数,且 $r\geqslant 3, d\geqslant 1$. 平凡的例子有 $7=(2^3-1)/(2-1)=$

$(-3)^3-1)/((-3-1)$，但是，不存在另外的 $<10^{10}$ 的这样的素数. 如果 p 是素数的条件放宽，则该问题便回到 Goormaghtigh 问题上去了，且有解 $8191=(2^{13}-1)/(2-1)=(90^3-1)/(90-1)$. 设 N 是任意正整数，$s(N)$ 表示方程 $N=1+x+x^2+\cdots+x^y(y\geqslant 2)$ 的正整数解的个数，则有一个至今没有解决的猜想：除 $N=31$，8191 外必有 $s(N)\leqslant 1$. Shorey 证明了，当 y 为偶且 $N-1$ 含有至多 5 个不同素因子时，猜想正确. 同时，他还证明了：

$$s(N)\leqslant\begin{cases}\max(2\omega(N-1)-3,0),\text{当 }\omega(N-1)\leqslant 4,\\ 2\omega(N-1)-4,\text{其它}.\end{cases}$$

这里 $\omega(\quad)$ 表不同素因子的个数.

E. T. Parker 注意到，如果能证明 $(p^q-1)/(p-1)$ 不整除 $(q^p-1)/(q-1)$ 的话，其中 p,q 是不同的奇素数，则 Feit 和 Thompson 关于奇阶群是可解的冗长的证明可以缩短. 事实上，已有人这样猜想，这两个表达式是互素的. 但 Nelson M. Stephens 发现，当 $p=17,q=3313$ 时，他们有公因子 $2pq+1=112643$. Mckay 对 $p<53\times10^6$，证明了 $p^2+p+1\nmid 3^p-1$.

Erdös 问，使整数 $a_i(1\leqslant a_1<\cdots<a_k\leqslant n)$ 中没有 l 个两两互素的最大的 k 是多少. 他猜想，这个 k 便是不超过 n 且有前 $l-1$ 个素数中的一个作为其因子的整数个数. 他说，容易证明 $l=2$ 时的情形，证明 $l=3$ 时的情形也不困难. 但是，他为此猜想的一般解决提供 10 美元奖金.

相应地，人们欲求 $[1,n]$ 的最大子集，它的元素两两最小公倍不超过 n. 如 $g(n)$ 是这样最大子集的元素个数，则 Erdös 证明了：

$$\frac{3}{2\sqrt{2}}n^{1/2}-2<g(n)\leqslant 2n^{1/2},$$

其中，头一个不等式在取从1到 $(n/2)^{1/2}$ 和从 $(n/2)^{1/2}$ 到 $(2n)^{1/2}$ 的偶整数时均成立. Choi 改进上界到 $1.638n^{1/2}$.

[1]P. T. Bateman and R. M. Stemmler, Waring's problem for algebraic num-

ber fields and primes of the form$(p^r-1)/(p^d-1)$,*Illinois J. Math.*, 6(1962),142-156.

[2]S. L. G. Choi,The largest subset in $[1,n]$ whose integers have pairwise l. c. m. not exceeding n,*Mathematika*,19 (1972),221-230.

[3]S. L. G. Choi,On sequences containing at most three pairwise coprime integers, *Trans. Amer. Math. Soc.*,183(1973),437-440;*MR* 48#6052.

[4]Ted Chinburg and Melvin Henriksen,Sums of kth powers in the ring of polynomials with integer coefficients, *Bull. Amer. Math. Soc.*,81 (1975),107-110.

[5]P. Erdős, Extremal problems in number theory, *Proc. Sympos. Pure Math. Amer. Math. Soc.*,8(1965),181-189;*MR* 30#4740.

[6]Kenneth Lebensold,A divisibility problem, *Studies in Applied Math.*, 56(1976-77),291-294;*MR* 58#21639.

[7]A. Makowski and A. Schinzel,Sur l'équation indéterminée de R. Goormaghtigh, *Mathesis*,68(1959),128-142 and 70(1965),94-96.

[8]T. N. Shorey,Integers with identical digits, *Acta Arith.*, 53(1989),2: 187-205.

[9]N. M. Stephens, On the Feit-Thompson conjecture, *Math. Comp.*, 25(1971),625.

B22. $n+k$ 的除不尽 $n+i(0\leqslant i<k)$ 的素因子的个数

Erdős 和 Selfridge 定义 $v(n;k)$ 为 $n+k$ 的除不尽 $n+i(0\leqslant i<k)$ 的素因子的个数,$v_0(n)$ 为取遍所有 $k\geqslant 0$ 的 $v(n;k)$ 的最大值. 那么,$v_0(n)$ 随 n 趋向 ∞ 吗?他们证明,除开 1,2,3,4,7,8 和 16 外,对所有 n 均有 $v_0(n)>1$. 更一般地,定义 $v_l(n)$ 为 $v(n;k)$ 取遍 $k\geqslant l$ 的最大值,那么 $v_l(n)$ 随 n 趋向 ∞ 吗?甚至不能证明 $v_1(n)=1$ 仅有有限组解. 大概使 $v_1(n)=1$ 的最大 n 为 $n=330$.

他们还用 $V(n;k)$ 表 $p^a\|(n+k)$ 但 $p^a\nmid(n+i)(0\leqslant i<k)$ 的素数 p 的个数,用 $V_l(n)$ 表示取遍 $k\geqslant l$ 的 $V(n;k)$ 的最大值,那么,$V_1(n)=1$ 仅有有限组解吗?也许 $n=80$ 是最大的解. 使 $V_0(n)=2$ 成立的最大的 n 是多少?

他们的论文还给出了若干更进一步的问题.

[1]P. Erdös and J. L. Selfridge, Some problems on the prime factors of consecutive integers, *Illinois J. Math.*, 11(1967), 428-430.
[2]A. Schinzel, Unsolved problem 31, *Elem. Math.*, 14(1959), 82-83.

B23. 连续数因子问题

Selfridge 问,存在 n 个连续整数,每一个都有 $<n$ 的两个不同素因子或相同素因子吗?他给出两个例子:

$a)$ $a+11+i(1\leqslant i\leqslant n=115)$,其中 $a\equiv 0(\bmod 2^2\times 3^2\times 5^2\times 7^2\times 11^2)$ 且对每个素数 p, $13\leqslant p\leqslant 113$ 有 $a+p\equiv 0(\bmod p^2)$.

$b)$ $a+31+i(1\leqslant i\leqslant n=1329)$,其中对于每一个 p, $37\leqslant p\leqslant 1327$ 有 $a+p\equiv 0(\bmod p^2)$ 且 $a\equiv 0(\bmod 2^2\times 3^2\times 5^2\times 7^2\times 11^2\times 13^2\times 17^2\times 19^2\times 23^2\times 29^2\times 31^2)$.

很难找到这样的 n 个连续数,其中每一个均能被小于 n 的两个不同素数或小于 $n/2$ 的一个素数的平方整除,尽管 Selfridge 相信用计算机能找到这样的数.

这与下面的问题有关:找到 n 个连续整数,每一个均有一个其他 $n-1$ 个数乘积的复合因子.如果放宽复合条件,仅求比 1 大的因子,则 $2184+i(1\leqslant i\leqslant n=17)$ 是一个著名的例子.

Erdös, Graham 和 Selfridge 希望找到最小的 t_n,使整数 $n, n+1,\cdots,n+t_n$ 的子集中的元素乘积为平方数(此子集至少应有两个元素).Thue-Siegel 定理推出当 $n\to\infty$ 时 $t_n\to\infty$ 的速度远比 $(\ln n)^c$ 的快,这里 c 是正常数.

换句话说,对每个 c,存在 n_0 使对于每一个 $n>n_0$, $\prod a_i$ 取遍 $n<a_1<\cdots<a_k<n+(\ln n)^c(k=1,2,\cdots)$ 的值都是不同的吗?他们证明了,对于 $c<2$, 上述为真.

关于连续数的 Grimm 猜想见 B25.

[1] Alfred Brauer, On a property of k consecutive integers, *Bull. Amer. Math. Soc.* 47(1941), 328-331; *MR* 2, 248.

[2] Ronald J. Evans, On blocks of N consecutive integers, *Amer. Math. Monthly* 76(1969), 48-49.

[3] Ronald Evans, On N consecutive integers in an arithmetic progression, *Acta Sci. Math. Unic. Szeged*, 33(1972), 295-296.

[4] Heiko Harborth, Eine Eigenschaft aufeinanderfolgender Zahlen, *Arch. Math.* (basel), 21(1970), 50-51.

[5] Heiko Harborth, Sequenzen ganzer Zahlen, in *Zahlentheorie, Berichte aus dem Math. Forschungsinst. Oberwolfach*, 5(1971)59-66.

[6] S. S. Pillai, On m consecutive integers I, *Proc. Indian Acad. Sci.* Sect A, 11(1940)6-12; *MR* 1, 199; II *ibid*, 11(1940)73-80; *MR* 1, 291; III *ibid*, 13(1941), 530-533; *MR* 3, 66; IV *Bull. Calcutta Math. Soc.* 36(1944), 99-101; *MR* 6, 170.

B24. 二项式系数

Earl Ecklund, Roger Eggleton, Erdös 和 Selfridge 记二项式系数 $\binom{n}{k}=n!/k!(n-k)!$ 为积 UV，这里 U 的每一个素因子至多为 k，而 V 的每个素因子均大于 k. 当 $n\geqslant 2k$ 时，仅有有限多种情形使 $U>V$，试确定 $k=3,5$，或 7 时的所有这些情形.

S. P. Khare 列出了 $n\leqslant 551$ 时的全部情形：$k=3, n=8, 9, 10, 18, 82$ 和 162；$k=5, n=10, 12$ 和 28；$k=7, n=21, 30$ 和 54.

Erdös 还注意到，对 $n>4$，仍不清楚 $\binom{2n}{n}$ 是否是无平方因子. 设 $e=e(n)$，这里 e 满足 $p^e\|\binom{2n}{n}$，现也不知道是否 e 随 n 趋向 ∞. 另一方面，他否定不了 $e>c\ln n$.

Wolstenholme 定理告诉我们，如果 n 是大于 3 的素数，那么 $\binom{2n-1}{n}\equiv 1 \pmod{n^3}$. James P. Jones 问是否逆命题也成立.

关于二项式系数$\binom{n}{k}=n!/k!(n-k)!$的小于n的最大因子，Erdős 指出，很容易证明，它至少是n/k，并且猜想，对于任何$c<1$和充分大的n，在cn和n之间也许存在一个这样的最大因子. Marilyn Faulkner 证明，如果p是$>2k$的最小素数，且$n\geqslant p$，则除开$\binom{9}{2}$和$\binom{10}{3}$外，$\binom{n}{k}$有一个$\geqslant p$的素因子. Earl Ecklund 证明了，如果$n\geqslant 2k>2$，则$\binom{n}{k}$除开$\binom{7}{3}$外，有素因子$p\leqslant n/2$.

John Selfridge 猜想，如果$n\geqslant k^2-1$，那么，除了例外情形$\binom{62}{6}$，$\binom{n}{k}$必存在一个$\leqslant n/k$的素因子. 在另一个方面，他猜想，如果$n<k(k+3)$，则除开$\binom{7}{3}$，$\binom{14}{4}$，$\binom{23}{5}$，$\binom{44}{8}$和$\binom{47}{11}$外，$\binom{n}{k}$有一个$\leqslant k+1$的素因子. 如果猜想条件减弱为$n\leqslant k+3$，则这些例外也将被包括进去.

由 Sylvester 和 Schur 独立发现的一个经典定理知，k个比k大的连续整数的积必有比k大的素因子. Leo Moser 猜想，Sylvester—Schur 定理对于素因子$\equiv 1 \pmod 4$成立，也就是说，k个比k大的连续整数之积有大于k的素因子$\equiv 1 \pmod 4$. 可是，Erdős 认为此猜想不成立.

Neil Sloane 注意到$\frac{3}{5m+3}\binom{5m+3}{m}$总是整数且问推广到$\frac{a}{n}\binom{n}{r}$的情况如何. 从 Catalan 数$\frac{1}{n+1}\binom{2n}{n}$知，这种推广可能是存在的.

$f(n)$是不能除尽$\binom{2n}{n}$的小于n的那些素数的倒数和. Erdős 等人猜想，必存在绝对常数c，使$f(n)<c$对所有n成立. Erdős 也猜想，对$n>4$，$\binom{2n}{n}$决不是无平方因子. 因为除$n=2^k$，均有$4\mid\binom{2n}{n}$，故仅需考虑$\binom{2^{k+1}}{2^k}$就足够了.

Erdős 又猜想,对 $k > 8$, 2^k 不是 3 的不同幂的和[$2^8 = 3^5 + 3^2 + 3 + 1$]. 如果这为真,则对 $k \geqslant 9$, 有 $3 \mid \binom{2^{k+1}}{2^k}$. $\binom{342}{171}$ 是 $\binom{2n}{n}$ 中不能被奇素数的平方除尽的最大数吗?

Graham 为 $\left(\binom{2n}{n}, 105\right) = 1$ 是否出现无穷多次这一问题的解决提供100美元的奖金. Kummer 知道,当满足这一条件的 n 用3,5或7进制表示时, n 将分别仅有数字:0,1;0,1,2;或0,1,2,3. H. Gupta 和 S. P. Khare 找到了小于7^{10}的14个这样的 n 值:1,10,756,757, 3160, 3186, 3187, 3250, 7560, 7561, 20007, 59548377 和 59548401. Peter Montgomery,Khare 和其他人找到了许多更大一些的 n.

Graham,Erdős,Ruzsa 和 Straus 证明了,对于任意的两个不同素数 p,q,存在无穷多个 n 使$\left(\binom{2n}{n}, pq\right) = 1$.

如果 $g(n)$ 是$\binom{2n}{n}$的最小素因子,那么 $g(3160) = 13$ 且对于 $3160 < n < 10^{110}$ 有 $g(n) \leqslant 11$.

如果 $H_{k,n}$ 是这样一个命题,存在某个 i, $0 \leqslant i < k$ 使 $n - i$ 除尽 $\binom{n}{k}$. 那么 Erdős 问,当 $n \geqslant 2k$ 时, $H_{k,n}$ 是否对所有 k 为真?Schinzel 给出了一个反例: $n = 99215$, $k = 15$. 如果 H_k 表示 $H_{k,n}$ 对所有 n 为真的命题,那么 Schinzel 证明了对于 $k = 15,21,22,33,35,45,55,63,65,69,75,77,85,87,91,93,95$和99, H_k 均是错的. Schinzel 问是否存在无穷多个这样的 k, Erdős 证明了它的存在性. Schinzel 对所有的其他 $k \leqslant 32$,证明了 H_k 为真,并问,是否存在无穷多个 k,它不是素数幂,使得 H_k 为真. 他猜想不存在.

[1]E. F. Ecklund, On prime divisors of the binomial coefficient, *Pacific J. Math.* 29(1969)267-270.

[2]P. Erdős, A theorem of Sylvester and Schur, *J. London Math. Soc.*, 9(1934), 282 − 288.

[3]Paul Erdős, A mélange of simply posed conjectures with frustratingly elusive solutions, *Math. Mag.*, 52(1979), 67-70.

[4]P. Erdős and R. L. Graham, On the prime factors of $\binom{n}{k}$, *Fibonacci Quart.* 14(1976), 348-352.

[5]P. Erdős, R. L. Graham, I. Z. Ruzsa, and E. Straus, On the prime factors of $\binom{2n}{n}$, *Math. Comp.*, 29(1975), 83-92.

[6]P. Erdős and G. Szekeres, Some number theoretic problems on binomial coefficients, *Austral. Math. Soc. Gaz.*, 5(1978), 97-99; *MR* 80e: 10010.

[7]M. Faulkner, On a theorem of Sylvester and Schur, *J. London Math. Soc.*, 41(1966), 107-110.

[8]L. Moser, Insolvability of $\binom{2n}{n} = \binom{2a}{a}\binom{2b}{b}$, *Canad. Math. Bull.*, 6(1963), 167-169.

[9]A. Schinzel, Sur un probléme de P. Erdős, *Colloq. Math.*, 5(1957-58)198-204.

[10]I. Schur, Einige Sätze über Primzahlen mit Anwendungen and Irreduzibilitätsfragen I, *S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl.* 14(1929), 125-136.

[11]J. Sylvester, On arithmetical series, *Messenger of Math.*, 21(1892)1-19, 87-120.

[12]W. Utz, A conjecture of Erdős concerning consecutive integers, *Amer. Math. Monthly*, 68(1961), 896-897.

B25. **Grimm 猜想**

Grimm 猜想，如果 $n+1, n+2, \cdots, n+k$ 都是合数，那么存在不同素数 p_{i_j}，使 $p_{i_j} \mid (n+j)(1 \leqslant j \leqslant k)$ 成立. 例如

1802，1803，1804，1805，1806，1807，1808，1809 和 1810

能够分别被

$$53,601,41,19,43,139,113,67 \text{ 和 } 181$$

除尽，而

114，115，116，117，118，119，120，121，122，123，124，125 和 126

各自能被 19，23，29，13，59，17，2，11，61，41，31，5 和 7 整除.

Erdős 和 Selfridge 欲求 $f(n)$ 的估计，这里 $f(n)$ 取最小数，使对每一个 m，在$[m+1, m+f(n)]$ 中有不同的整数 $a_1, a_2, \cdots, a_{\pi(n)}$ 满足 $p_i | a_i$，其中 p_i 是第 i 个素数. 他们俩与 Pomerance 证明了对于大 n 有

$$(3-\varepsilon)n \leqslant f(n) \ll n^{3/2}(\ln n)^{-1/2}.$$

[1]P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, *Congressus Numerantium* XXI in *Proc. 9th S. E. Conf. Combin. Graph Theory, Comput.*, Boca Raton, Utilitas Math. Winnipeg, 1978, 29-40.

[2]P. Erdős and C. Pomerance, Matching the natural numbers up to n with distinct multiples in another interval, *Nederl. Akad. Wetensch. Proc. Ser.* A 83(= *Indag. Math.* 42)(1980), 147-161.

[3]Paul Erdős and Carl Pomerance, An analogue of Grimm's problem of finding distinct prime factors of consecutive integers, *Utilitas Math.*, 19(1981).

[4]P. Erdős and J. L. Selfridge. Some problems on the prime factors of consecutive integers II, in *Proc. Washington State Univ. Conf. Number Theory*, Pullman, 1971, 13-21.

[5]C, A. Grimm, A conjecture on consecutive composite numbers, *Amer. Math. Monthly*, 76(1969), 1126-1128.

[6]Michel Langevin, Plus grand facteur premier d'entiers en progression arithmétique, sém. Delange-Pisot-Poitou, 18(1976/77) Théorie des nombres, Fasc. 1, Exp. No. 3(1977); *MR* 81a; 10011.

[7]Carl Pomerance, Some number theoretic matching problems, in *Proc. Number Theory Conf.*, Queens Univ., Kingston, 1979, 237-247.

[8]K. T. Ramachandra, N. Shorey, and R. Tijdeman, On Grimm's problem

relating to factorization of a block of consecutive integers, *J. reine angew. Math.*, 273(1975), 109-124.

B26. 连续数之积的相同素因子

假设$f(n)$是这样的最小整数，它使得$n, n+1, \cdots, n+f(n)$中至少有一个能除尽其他数之积. 很容易看出，$f(k!)=k$，且对$n>k!$有$f(n)>k$. Erdős 证明了：

$$f(n)>\exp((\ln n)^{1/2-\epsilon})$$

对于无穷多的n成立，但似乎很难找到$f(n)$的一个好的上界.

Erdős 问，当$k\geqslant l\geqslant 3$时，$(m+1)(m+2)\cdots(m+k)$与$(n+1)(n+2)\cdots(n+l)$是否无穷多次地含相同的素因子.

例如，$2\times3\times4\times5\times6\times7\times8\times9\times10$，$14\times15\times16$与$48\times49\times50$，还有$2\times3\times4\times5\times6\times7\times8\times9\times10\times11\times12$与$98\times99\times100$. 对$k=l\geqslant3$，他猜想，这仅发生有限多次.

如果$L(n;k)$是$n+1, n+2, \cdots, n+k$的最小公倍数，那么，Erdős 猜想，对$l>1, n\geqslant m+k, L(m;k)=L(n;l)$仅有有限个解. 他问是否存在无限多个$n$使对所有$k(1\leqslant k<n)$，我们有$L(n;k)>L(n-k;k)$. 使此不等式反号的最大$k=k(n)$是多少？他注意到，极易看出$k(n)=o(n)$，而且认为这可能是正确的. 他预测，对每个$\epsilon>0$和$n>n_0(\epsilon)$，有$k(n)<n^{1/2+\epsilon}$成立，但是不能证明它.

[1]P. Erdős, How many pairs of products of consecutive integers have the same prime factors? *Amer. Math. Monthly*, 87(1980), 391-392.

B27. Euler 函数

Euler 函数$\varphi(n)$是不大于n且与n互素的正整数的个数，例如，$\varphi(1)=\varphi(2)=1, \varphi(3)=\varphi(4)=\varphi(6)=2, \varphi(5)=\varphi(8)=\varphi(10)=\varphi(12)=4, \varphi(7)=\varphi(9)=6$. 那么，存在无穷多对相邻数$n, n+1$使$\varphi(n)=\varphi(n+1)$成立吗？例如，$n=1, 3, 15, 104, 164, 194, 255$,

495,584,975 均有 $\varphi(n)=\varphi(n+1)$. 但是我们不知道 $|\varphi(n+1)-\varphi(n)|<n^{\varepsilon}$ 是否对每一个 $\varepsilon>0$ 有无穷多组解?

Schinzel 猜想,对于每一偶数 k,方程 $\varphi(n+k)=\varphi(n)$ 有无穷多组解. 他注意到,k 为奇时的对应的猜想是不可信的. 对 $k=1$,在 $n<10^4$ 时,$\varphi(n+k)=\varphi(n)$ 有 18 个解. 而对 $k=3$,在同样范围内仅有两个解 $n=3$ 和 $n=5$. D. H. Lehmer 把范围推到 $n<10^6$,且对 $k=1$,找到 59 个解,但对 $k=3$,仅找到两个. Sierpinski 已证明,对每一个 k 值,$\varphi(n+k)=\varphi(n)$ 至少有一个解. Schinzel 和 Wakulicz 证明,对于 $k<2\times10^{58}$,对每个 k 方程至少有2个解. Makowski 证明,对每个 k 方程 $\varphi(n+k)=2\varphi(n)$ 至少有一个解.

两个奇特的情形是 $\varphi(25930)=\varphi(25935)=\varphi(25940)=\varphi(25942)=2^7 3^4$ 及 $\varphi(404471)=\varphi(404473)=\varphi(404477)=2^8\cdot 3^2\cdot 5^2\cdot 7$.

设 n 为正整数,如果 $\varphi(x)=n$ 没有解,则称 n 是 Nontotients. 例如 $n=14,26,34,38,50,62,68,74,76,86,90,94,98$ 均是 Nontotients. Lehmer 计算出小于 y 的 Nontotients 的个数 #(y)如下:

y	10^3	10^4	2×10^4	3×10^4	4×10^4	5×10^4	6×10^4	7×10^4	8×10^4	9×10^4
#(y)	210	2627	5515	8458	11438	14439	17486	20536	23606	26663

设 n 为正整数,如果方程 $x-\varphi(x)=n$ 无解,则称 n 为 Noncototients 数. 例如 $n=10,26,34,50,52,58,86,100$ 均是 Noncototients 数.Sierpinski 和 Erdös 猜想,存在无穷多个Noncototiens 数.

[1]P. Erdös, Über die Zahlen der Form $\sigma(n)-n$ and $n-\varphi(n)$, *Elem. Math.*, 28(1973), 83-86.

[2]Andrzej Makowski, On the equation $\varphi(n+k)=2\varphi(n)$, *Elem. Math.*, 29(1974), 13

[3]A. Schinzel, Sur l' équation $\varphi(x+k)=\varphi(x)$, *Acta Arith.*, 4(1958),

181-184; *MR* 21 # 5597.

[4] A. Schinzel and A. Wakulicz, Sur l'équation $\varphi(x+k)=\varphi(x)$ Ⅱ, *Acta Arith.*, 5(1959), 425-426; *MR* 23 # A831.

[5] W. Sierpinski, Sur un propriété de la fonction $\varphi(n)$, *Publ. Math. Debrecen*, 4(1956), 184-185.

B28. **Lehmer 猜想**

D. H. Lehmer 猜想，不存在合数 n，使得 $\varphi(n)$ 为 $n-1$ 的因子. 也就是说，不存在 n 使 $\varphi(n)$ 为 $n-1$ 的真因子. 这样的 n 必定是 Carmichael 数(A13). D. H. Lehmer 证明了，如果 $\varphi(n)$ 为 $n-1$ 的真因子，则 n 至少是 7 个不同奇素数之积. 柯召和孙琦证明了 n 至少是 12 个不同的奇素数之积. Lieuwens 已证明了下列定理，如 $3|n$ 那么 n 至少有 212 个不同素因子且 $n>5.5\times10^{571}$；如果 n 的最小素因子至少为 7，那么 n 至少是13个素数之积. 这就取代并改正了 Schuh 的工作. Masao Kishore 已证明无论如何需要13个素数. Cohen 和 Hagis 则改进此结果到14. Pomerance 已证明，小于 x 且使 $\varphi(n)|(n-1)$ 的合数 n 的个数小于 $x^{1/2+\epsilon}$. 最近，Hagis Jr. 证明了以下结果：(a)如果 $3|n$，那么 n 至少有 298848 个不同素因子，且 $n>10^{1937042}$；(b) 如果 $M\geqslant3$，这里 M 是满足 $M\varphi(n)=n-1$ 的正整数，那么 n 至少有 1991 个不同素因子且 $n>10^{8171}$；(c) $S(M,t)$ 是一个有限集合，其中 $S(M,t)$ 是 n 的集合，n 满足：(1) n 恰有 t 个不同素因子；(2) $M\varphi(n)=n-1$ 有一个解 n.

Schinzel 注意到，如果 $n=p$ 或 $2p$，其中 p 为素数，则 $\varphi(n)+1$ 除尽 n，并问逆命题是否常真？

如果 n 是素数，那么 n 除尽 $\varphi(n)d(n)+2$. 除开 $n=4$，它对任意合数 n 均为真吗？Subbaro 也注意到，如果 n 为素数，及 $n=4,6,22$，则 $n\sigma(n)\equiv2(\mathrm{mod}\ \varphi(n))$. 它对无穷多个 n 为真吗？曹珍富给出了一个否定的回答，即证明了 $n\sigma(n)\equiv2(\mathrm{mod}\ \varphi(n))$ 当且仅当 $n=4,6,22$ 及 n 是一个素数.

Subbarao 基于函数 $\varphi^*(n) = \prod(p^a - 1)$，作了一个与 Lehmer 类似的猜想，其中 $\prod$ 跑遍除尽 n 的最大素数幂，即 $p^a \| n$. 他猜想，如 $\varphi^*(n) | (n-1)$，则 n 是某素数的幂.

Ron Graham 作了下列猜想：

对每个 k，存在无穷多个 n 使 $\varphi(n) | (n-k)$？他注意到，它对 $k = 0, k = 2^a (a \geqslant 0)$ 及 $k = 2^a 3^b (a, b > 0)$ 为真.

[1]Ronald Alter, Can $\varphi(n)$ properly divide $n-1$? *Amer. Math. Monthly*, 80(1973), 192-193.

[2]Graeme L. Cohen and Peter Hagis, On the number of prime factors of n if $\varphi(n) | (n-1)$, *Nicuw Arch. Wisk.* (3)28(1980), 177-185.

[3]Peter Hagis Jr., On the equation $M\varphi(n) = n - 1$, *Nieuw Arch. Wisk.* (4)6(1988), 3: 255-261.

[4]Masao Kishore, On the equation $k\varphi(M) = M - 1$, *Nieuw Arch. Wisk.* (3)25(1977), 48-53. See also *Notices Amer. Math. Soc.*, 22(1975) A. 501-502.

[5]柯召(C. Ko)，孙琦，关于方程 $k\varphi(n) = n - 1$，四川大学学报(自然科学版)，1(1963)，13

[6]D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.*, 38(1932), 745-751.

[7]E. Lieuwens, Do there exist composite numbers for which $k\varphi(M) = M - 1$ holds? *Nieuw Arch. Wisk.* (3)18(1970), 165-169; *MR* 42#1750.

[8]C. Pomerance, On composite n for which $\varphi(n) | n - 1$, *Acta Arith.*, 28(1976), 387-389; *II*, *Pacific J. Math*, 69(1977), 177-186. See also *Notices Amer. Math. Soc.*, 22(1975) A-542.

[9]Fred Schuh, Can $n - 1$ be divisible by $\varphi(n)$ where n is composite? *Mathematica*, Zutphen B. 12(1944), 102-107.

[10]M. V. Subbarao, On two congruences for primality, *Pacific J. Math.*, 52(1974), 261-268; *MR* 50#2049.

[11]David W. Wall, Conditions for $\varphi(N)$ to properly divide $N - 1$, *A Collection of Manuscripts Related to the Fibonacci Sequence*, 18th An-

niv. Vol. ,Fibonacci Assoc. 205-208.

B29. $\varphi(m)=\sigma(n)$与$\varphi(m)=\varphi(n)$

存在无穷多对数 m,n 使 $\varphi(m)=\sigma(n)$ 吗?因为对素数 p,$\varphi(p)=p-1$ 和 $\sigma(p)=p+1$,所以如果存在无穷多的孪生素数(A7),那么该问题的回答是肯定的.又如果存在无穷多的 Mersenne 素数(A3) $M_p=2^p-1$,那么 $\sigma(M_p)=2^p=\varphi(2^{p+1})$.但是,除开这些,有时候还存在许多不曾被人们注意到的解的形式,如 $\varphi(780)=192=\sigma(105)$.

Erdős 评论说,方程 $\varphi(x)=n!$ 是可解的,并且(除开 $n=2$) $\sigma(y)=n!$ 也是可解的.

Carmichael 猜想,对每一个 n,似乎可能找到不等于 n 的 m 使得 $\varphi(m)=\varphi(n)$ 成立,并且于本世纪初,人们曾认为此猜想已被 Carmichael 证明. Klee 证明该猜想对全部不被 $2^{42}\times 3^{47}$ 除尽的 n 和 $\varphi(n)<10^{400}$ 时成立. Pomerance 证明了,如果 n 满足对于每一素数 p,$p-1$ 能除尽 $\varphi(n)$,且我们有 p^2 除尽 n,则 n 是一个反例.他又能证明(未发表)由 Schinzel 的头一个素数 $p\equiv 1 \pmod q$ 小于 q^2 的猜想可推出不存在 n 满足他的定理.

Erdős 证明,如果 $\varphi(x)=k$ 恰有 s 个解,则存在无穷多个 k 恰有 s 个解,且 $s>k^c$ 对于无穷多个 k 成立.如果 C 是使不等式为真的那些 C 中最小上界,则 Wooldridge 证明了 $C\geqslant 3-2\sqrt{2}>0.17157$. Pomerance 用 Hooley 对 Brun-Titchmarsh 定理的改进结果改进它为 $C\geqslant 1-625/512e>0.55092$,且注意到,由 Iwaniec 最近作出的进一步改进使他得到 $C>0.55655$,从而 $s>k^{5/9}$ 对于无穷多个 k 成立. Erdős 猜想 $C=1$.另一方面,Pomerance 又证明了 $s<k\exp\{-(1+o(1))\ln k\ln\ln\ln k/\ln\ln k\}$,并给出了此结果为可能达到的最好结果的直观推断.

[1]R. D. Carmichael, Note on Euler's φ-function, *Bull. Amer. Math. Soc.*,

28(1922),109-110.

[2]P. Erdös, on the normal number of prime factors of $p-1$ and some other related problems concerning Euler's φ-function, *Quart. J. Math. Oxford Ser.* 6(1935),205-213.

[3]P. Erdös, Some remarks on Euler's φ-function and some related problems, *Bull. Amer. Math. Soc.*, 51(1945),540-544.

[4]P. Erdös, Some remarks on Euler's φ function, *Acta Arith.*, 4(1958), 10-19; *MR* 22#1539.

[5]P. Erdös and R. R. Hall, Distinct values of Euler's φ-function, *Mathematika*, 23(1976),1-3.

[6]C. Hooley, On the greatest prime factor of $p+a$, *Mathematika*, 20(1973),135-143.

[7]V. L. Klee, On a conjecture of Carmichael, *Bull. Amer. Math. Soc.*, 53(1947),1183-1186; *MR* 9,269.

[8]V. L. Klee, Is there an n for which $\varphi(x)=n$ has a unique solution? *Amer. Math. Monthly*, 76(1969),288-289.

[9]Carl Pomerance, On Carmichael's conjecture, *Proc. Amer. Math. Soc.*, 43(1974),297-298.

[10]Carl Pomerance, Popular values of Euler's function, *Mathematika* 27(1980),84-89.

[11]K. R. Wooldridge, Values taken many times by Euler's phi-function, *Proc. Amer. Math. Soc.*, 76(1979),229-234; *MR* 80g:10008.

B30. 小于 n 且与它互素的整数间隔

如果 $a_1<a_2<\cdots<a_{\varphi(n)}$ 是小于 n 且与它互素的整数，Erdös 猜想，$\sum(a_{i+1}-a_i)^2<cn^2/\varphi(n)$ 并为这一猜想的解决提供100美元的奖金. Hooley 证明，对于 $1\leqslant\alpha<2$，$\sum(a_{i+1}-a_i)^\alpha\ll n(n/\varphi(n))^{\alpha-1}$ 和 $\sum(a_{i+1}-a_i)^2\ll n(\ln\ln n)^2$. 而 Vaughan 已证得

$$\sum(a_{i+1}-a_i)^2\ll n^2(1+\sum_{p\mid n}(\ln p)/p)/\varphi(n),$$

因而“在通常情形”证实了这一猜想.

Jacobsthal 问 $\max(a_{i+1}-a_i)$的上界是什么？

[1]P. Erdős, on the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal, *Math. Scand.*, 10(1962), 163-170; *MR* 26#3651.

[2]C. Hooley, On the difference of consecutive numbers prime to n, *Acta Arith.*, 8(1963), 343-347.

[3]R. C. Vaughan, Some applications of Montgomery's sieve, *J. Number Theory*, 5(1973), 64-79.

B31. φ 与 σ 的叠代

因子和与酉因子和间存在一个紧密联系的函数，该函数是 Euler 函数的补充. 如果 $n=p_1^{a_1}\cdots p_k^{a_k}$，且用 $\bar{\varphi}(n)$ 表 $\prod p_i^{a_i-1}(p_i+1)$，即 $\bar{\varphi}(n)=n\prod(1+p^{-1})$，其中积跑遍 n 的不同素因子. 易知，此函数的叠代最终趋于的项具有 $2^a\times 3^b$ 形式，其中 b 固定，a 逐项增 1. 任意给定 b 值，存在无穷多的 n 初值使叠代最终趋向 $2^a\times 3^b$. 例如，$\bar{\varphi}^k(2^a\times 3^b\times 7^c)=2^{a+4k}\times 3^b\times 7^{c-k}(0\leqslant k\leqslant c)$ 和 $\bar{\varphi}^k(2^a\times 3^b\times 7^c)=2^{a+5k-c}\times 3^b(k>c)$.

David E. Penney 和 Pomerance 在一篇未发表的文章中，证明了存在 n 使函数 $\bar{\varphi}(n)-n$ 的叠代当叠代次数趋于 ∞ 时无界. 最小的这样的数 $n=318$.

如果我们用$(\varphi+\bar{\varphi})/2$ 来求 $\bar{\varphi}$ 和 φ 平均并进行叠代，那么当叠代到某一步为素数幂时叠代序列的项便变成了常数. 例如对 24，我们有 $\frac{1}{2}(8+48)=2$，$\frac{1}{2}(12+48)=30$，$\frac{1}{2}(8+72)=40$，$\frac{1}{2}(16+72)=44$，$\frac{1}{2}(20+72)=46$，$\frac{1}{2}(22+72)=47$，$\frac{1}{2}(46+48)=47$，… 还有其他的无穷递增的数吗？

我们也能取 σ 和 φ 的平均 $\frac{1}{2}(\sigma+\varphi)$ 并进行叠代. 因为 $\varphi(n)$ 对于 $n>2$ 总为偶数且当 n 是一个平方数或平方数的 2 倍时，$\sigma(n)$ 总

为奇. 因此有时我们将得到一些非整数值. 例如 54,69,70,84,124,142,143,144,225 $\frac{1}{2}$;在这种情形下,我们说序列是断裂的. 容易证明,仅仅当 $n=1$,或是素数时,$(\sigma(n)+\varphi(n))/2=n$,因此,序列能变成常数,例如 60,92,106,107,107,… 再一次问,存在其他的数能产生无穷递增的序列吗?

当然,如果我们叠代 φ 函数,那么它最终将到达 2,称使 $\varphi^k(n)=2$ 的整数 k 为 n 的类.

k	n														
0	2														
1	3	4	6												
2	5	7	8	9	10	12	14	18							
3	11	13	15	16	19	20	21	22	24	26	…				
4	17	23	25	29	31	32	33	34	35	37	39	40	43	…	
5	41	47	51	53	55	59	61	64	65	67	68	69	71	73	…
6	83	85	89	97	101	103	107	113	115	119	121	122	123	125	128 …

$M=\{2,3,5,11,17,41,83,\cdots\}$ 是这些类最小值的集合. Shapiro 猜想,M 仅含有素数值,但是 Mills 却找到几个合数元素. 如果 S 是对于全部 k,类 k 的小于 2^{k+1} 的元素的并,即:

$S=\{3;5,7;11,13,15;17,23,25,29,31;41,47,51,53,55,59,61;83,85,\cdots\}$,

则 Shapiro 证明了,S 的元素的因子也在 S 中. Catlin 证明了,如果 m 是 M 的奇元素,那么 m 的因子也属于 M,且仅仅当 M 中存在有限多个奇数时,M 中也存在有限多个素数. S 中含有无穷多个奇数吗? M 中含有无穷多个奇数吗?

Finucane 叠代函数 $\varphi(n)+1$,并问:经过多少步后,它才到达一个素数?此外,给定一个素数 p,其序列以素数 p 结束的 n 值的分布如何?5,8,10,12 是以 5 结束的仅有的数吗?7,9,14,15,16,18,20,24,30 是仅有的以 7 结束的数码?

Erdős 就 $\sigma(n)-1$ 也问了类似的问题,它总是结束于某个素

数，还是无限地递增？在 $\sigma(n)-1$，$(\bar{\varphi}(n)+\varphi(n))/2$ 或 $(\varphi(n)+\sigma(n))/2$ 的叠代的任何一种情形，他都没有证明其增长速度是否比指数慢.

[1]P. A. Catlin, Concerning the iterated φ-function, *Amer. Math. Monthly*, 77(1970), 60-61.

[2] Paul Erdős and R. R. Hall, Euler's φ — function and its iterates, *Mathematika*, 24(1977), 173-177; *MR* 57#12356.

[3] W. H. Mills, Iteration of the φ-function, *Amer. Math. Monthly*, 50(1953), 547-549.

[4]C. A. Nicol, Some diophantine equations involving arithmetic functions, *J. Math. Anal. Appl.*, 15(1966), 154-161.

[5]Harold N. Shapiro, An arithmetic function arising from the φ-function, *Amer. Math. Monthly*, 50(1943), 18-30; *MR* 4, 188.

B32. $\varphi(\sigma(n))$与$\sigma(\varphi(n))$

Makowski 和 Schinzel 证明，$\limsup \varphi(\sigma(n))/n=\infty$，$\limsup \varphi^2(n)/n=\frac{1}{2}$ 和 $\liminf \sigma(\varphi(n))\leqslant\frac{1}{2}+\frac{1}{2^{34}-4}$. 他们问是否 $\sigma(\varphi(n))/n\geqslant\frac{1}{2}$ 对全部 n 成立？他们指出，甚至是否有 $\inf \sigma(\varphi(n))/n>0$ 也未被证明.

[1]A. Makowski and A. Schinzel, On the function $\varphi(n)$ and $\sigma(n)$, *Colloq. Math.*, 13(1964-65), 95-99.

B33. 阶乘的"和"

数

$$3!-2!+1!=5$$
$$4!-3!+2!-1!=19$$
$$5!-4!+3!-2!+1!=101$$

$$6!-5!+4!-3!+2!-1!=619$$

$$7!-6!+5!-4!+3!-2!+1!=4421$$

$$8!-7!+6!-5!+4!-3!+2!-1!=35899$$

是素数. 存在无穷多个这样的素数吗?这里对下列几个 n 值列出 $A_n=n!-(n-1)!+(n-2)!-\cdots-(-1)^n 1!$ 的因子.

n	A_n	n	A_n
9	79×4139	19	15578717622022981(prime)
10	3301819(prime)	20	8969×210101×1229743351
11	13×2816537	21	113×167×4511191×572926421
12	29×15254711	22	79×239×56947572104043899
13	47×1427×86249	23	85439×289993909455734779
14	211×1679×229751	24	12203×24281×2010359484638233
15	1226280710981(prime)	25	59×555307×455254005662640637
16	53×6581×56470483	26	1657×234384986539153832538067
17	47×7148742955723	27	127^2×271×1163×2065633479970130593
18	2683×2261044646593	28	61×221171×21820357757749410439949

例 $n=27$ 的情形表明,A_n 不一定是无平方因子的.

如果存在 n 值使 $n+1$ 除尽 A_n,那么 $n+1$ 对于全部 $m>n$ 将除尽 A_m,因而仅有有限个素数值. Wagstaff 证明,如有这样的 n,则它必大于46340.

D. Kurepa 定义 $!n=0!+1!+\cdots+(n-1)!$ 并问对所有 $n>2$,是否有 $!n\not\equiv 0 \pmod n$. Slavic 利用计算机在 $3\leqslant n\leqslant 1000$ 时证明了 $!n\not\equiv 0 \pmod n$. 猜想是 $(!n,n!)=2$. Wagstaff 推广了 Slavic 的计算,并证实猜想在 $n<50000$ 时成立. 他注意到,对于 $B_n=!(n+1)-1=1!+2!+\cdots+n!$,我们有:当 $n\geqslant 2$ 时 $3|B_n$;当 $n\geqslant 5$ 时,$9|B_n$;当 $n\geqslant 10$ 时,$99|B_n$.

[1] L. Carlitz, A note on the left factorial function, *Math. Balkanica*, 5(1975)37-42.

[2] Duro Kurepa, On some new left factorial propositions, *Math. Balkanica*, 4(1974), 383-386; *MR* 58#10716.

B34. **Euler 数**

$\sec x = \sum E_n x^n/n!$ 的展开式中的系数是 Euler 数，且以几种组合的前后关系出现：$E_0 = 1, E_2 = -1, E_4 = 5, E_6 = -61, E_8 = 1385, E_{10} = -50521, E_{12} = 2702765, E_{14} = -199360981, E_{16} = 19391512145, E_{18} = -2404879675441, \cdots$. 对于任意素数 $p \equiv 1 \pmod 8$，$E_{(p-1)/2} \not\equiv 0 \pmod p$ 都为真吗？它对任意的 $p \equiv 5 \pmod 8$ 是正确的. 对于 $p \equiv 3 \pmod 4$，Mordell 证明：$E_{(p-3)/2} \not\equiv 0 \pmod p$ 的充要条件是 $y_0 \not\equiv 0 \pmod p$，y_0 是方程 $x^2 - py^2 = 1$ 的正整数解中最小的 y. Goldberg 证明了 $p < 18000$ 时 $y_0 \not\equiv 0 \pmod p$.

还有一个类似的问题是关于 Bernouilli 数的，参阅曹珍富的《丢番图方程引论》.

[1]曹珍富(Z. Cao)，丢番图方程引论，第五章 §7，哈尔滨工业大学出版社，1989.

[2]E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Annals of Math.*, 39(1938), 350-360; *Zbl.* 19, 5.

[3]L. J. Modell, *J. London Math. Soc.*, 36(1961), 282-288.

[4] Barry J. Powell, Advanced problem 6325, *Amer. Math. Monthly*, 87(1980), 826.

B35. **n 的最大素因子**

Erdős 用 $P(n)$ 表 n 的最大素因子，并且问是否存在无穷多个素数 p 使 $(p-1)/P(p-1) = 2^k$ 或 $= 2^k \cdot 3^l$ 成立？

Erdős 和 Pomerance 能证明，存在无穷多个 n 使 $P(n) < P(n+1) < P(n+2)$. 那么，存在无穷多个 n 使 $P(n) > P(n+1) > P(n+2)$ 吗？他们认为，渐近密率为 1/6 的 n 的集合满足条件.

[1]P. Erdős and Carl Pomerance, On the largest prime factors of n and $n+1$, *Aequationes Math.*, 17(1978), 311-321.

C 堆垒数论

C1. Goldbach 猜想

最为著名的问题之一便是 Goldbach 猜想，即每一大于 4 的偶数均能表为两奇素数之和. Vinogradov 证明了，每一比 $3^{3^{15}}$ 大的奇数均是三个素数之和，潘承彪给出了 Vinogradov 定理的一个很好的简化证明. 陈景润证明了，所有充分大的偶数均是一个素数与至多两素数乘积之和. 在这之前，王元与潘承洞作出了重要贡献，例如证明了：充分大的偶数均是一个素数与至多四个素数乘积之和. 潘承洞、丁夏畦与王元还给出陈景 润定理的一个简化证明.

Hardy 和 Littlewood(参见 A1，A8)的猜想 A 是：偶数 n 表为两奇素数和的表法个数 $N_2(n)$ 渐近地由下式给出：

$$N_2(n) \sim \frac{2cn}{(\ln n)^2}\prod \frac{p-1}{p-2},$$

其中，如同 A8，$2c \approx 1.3203$，积跑遍 n 的所有奇素因子.

M. L. Stein 和 P. R. Stein 已经计算了 $n < 10^5$ 时的 $N_2(n)$，找到了对所有 $k < 1911$ 使 $N_2(n) = k$ 的 n 值，他们猜想，$N_2(x)$ 取所有正整数.

设 $\pi(n;a,b)$ 表示 $a, a+b, a+2b, \cdots$ 中不超过 n 的素数个数，有一个均值定理是：设 $b \leqslant n^{\alpha}/(\ln n)^A$ 是正整数，$0 < \alpha < 1$，$A > 1$，如果

$$(A) \qquad \left|\pi(n;a,b) - \frac{n}{\varphi(b)\ln n}\right| < \frac{c}{(\ln n)^B}\prod \frac{p-1}{P-2},$$

这里 $B > 2$，$\varphi(b)$ 是 Euler 函数(B27)，那么

$$(B) \qquad N_2(n) \leqslant \frac{4cn}{\alpha(\ln n)^2}\prod \frac{p-1}{P-2}.$$

此处 c 与积均与前同. 显然,如果找到一个 α 使(A) 成立,则可得到 $N_2(n)$ 的一个上界. 1962年,潘承洞证明了在 $\alpha\leqslant 1/3$ 时(A) 成立. 而后潘承洞、Bombieri 和 Davenport 又分别得到 $\alpha\leqslant 3/8$,$\alpha\leqslant 1/2$,因而(B) 中 $4/\alpha$ 可取 8. 陈景润(1978) 给出 $4/\alpha$ 可取 7.8342.

设 $\varphi(n)$ 是 Euler 函数(B27),因此,如 p 是素数,则 $\varphi(p)=p-1$. 如果 Goldbach 猜想成立,则对一个数 m,必存在素数 p,q 满足

$$\varphi(p)+\varphi(q)=2m.$$

如果我们放宽 p,q 是素数的条件,那么,证明总有 p,q 满足上述方程就应当容易一些. Erdös 和 Leo Moser 问是否能做到这一点.

[1]E. Bombieri and H. Davenport, Small differences between prime number, *Proc. Roy. Soc.* Ser. A, 293(1966), 1－8.

[2]陈景润(J. R. Chen),大偶数表为一个素数与一个不超过两个素数的乘积之和,科学通报,17(1966),5:385－386;中国科学,16(1973),2:111－128;Ⅱ *Sci. Sin.*, 21(1978), 421－430.

[3]陈景润(J. Chen), On the Goldbach's problem and the sieve method, *Sci. Sin.*, 21(1978), 701－739.

[4]J. G. van der Corput, Sur l'hypothese de Goldbach pour presque tous les nombres pairs, *Acta Arith.*, 2(1937), 266-290.

[5]N. G. Cudakov, On the density of the set of even numbers which are not representable as the sum of two odd primes, *Izv. Akad. Nauk SSSR Ser. Mat.*, 2(1938), 25-40.

[6]N. G. Cudakov, On Goldbach-Vinogradov's theorem, *Ann. of Math.*, (2)48(1947), 515-545; *MR* 9, 11.

[7]T. Estermann, On Goldbach's problem: proof that almost all even positive integers are sums of two primes, *Proc. London Math. Soc.* (2)44(1938), 307-314.

[8]T. Estermann, Introduction to modern prime number theory, *Cambridge Tracts in Mathematics* 41, 1952.

[9]H. L. Montgomery and R. C. Vaughan, The exceptional set in Goldbach's problem, *Acta Arith.*, 27(1975), 353-370.

[10]潘承彪(C. B. Pan),三个素数定理的一个新证明,数学学报,20(1977),206—211.

[11]潘承洞(C. Pan),表偶数为素数及殆素数之和,数学学报,12(1962),95—106.

[12]潘承洞(C. D. Pan),丁夏畦(X. S. Ding),王元(Y. Wang),大偶数表为一个素数与一个殆素数之和,中国科学,18(1975),599-610; *MR* 57 # 5897.

[13]P. M. Ross, On Chen's theorem that each large even number has the form p_1+p_2 or $p_1+p_2p_3$, *J. London Math. Soc.* (2)10(1975),500-506.

[14]M. L. Stein and P. R. Stein, New experimental results on the Goldbach conjecture, *Math. Mag.*, 38(1965),72—80; *MR* 32# 4109.

[15]Robert C. Vaughan, On Goldbach's problem, *Acta Arith.*,22(1972),21 — 48.

[16] Robert C. Vaughan, A new estimate for the exceptional set in Goldbach's problem, *Proc. Sympos. Pure Math. Amer. Math. Soc.*, 24(Analytic Number Theory, St Louis,1972),315-319.

[17]I. M. Vinogradov, Representation of an odd number as the sum of three primes, *Dokl. Akad. Nauk SSSR*,15(1937),169-172.

[18]I. M. Vinogradov, Some theorems concerning the theory of primes, *Mat. Sb. N. S.* 2(44)(1937),179-195.

[19]王元(Y. Wang), On the representation of large integer as a sum of a prime and an almost prime, Sci. Sin.,11(1962),1033-1054.

[20]王元(Y. Wang),表大偶数为一个素数及一个不超过四个素数的乘积之和,数学学报,6(1956),565—582.

[21] Dan Zwillinger, A Goldbach conjecture using twin primes, *Math. Comp.*,33(1979),1071;*MR* 80*b*:10071.

C2. 幸运数

Gardiner 和其他人借助修改 Eratosthenes 筛法定义了幸运数,即从自然数中删去所有的偶数,而把奇数留下来,除开 1,头一个被留下来的数是 3,再从新序列中每隔 3—1 个删去一个(形如

$6k-1$ 的那些),留下

$$1,3,7,9,13,15,19,21,25,27,31,33,\cdots$$

下一个剩下来的数是 7,在这个序列中,每隔 7—1 个删去一个(数 $42k-23, 42k-3$). 下面 9 被剩下来了,因此,从剩下的数中每隔 9—1 个数删去一个,如此下去,直到得出全部的幸运数:

1,3,7,9,13,15,21,25,31,33,37,43,49,51,63,67,69,73,75,79, 87,93,99,105,111,115,127,129,133,135,141,151,159,163, 169,171,189,193,195,201,205,211,219,223,231,…

与关于素数的经典的问题平行,产生了许多与幸运数有关的问题,例如,如果 $L_2(n)$ 是 $l+m=n$ 解的个数,其中 n 是偶的,l,m 是幸运的,则 M. L. Stein 和 P. R. Stein 对所有 $k \leqslant 1769$,找到满足 $L_2(n)=k$ 的 n 值,且有一个与 C1 类似的猜想未能解决.

[1]W. E. Briggs,Prime-like sequences generated by a sieve process, *Duke Math. J.*,30(1963),297-312;*MR* 26#6145.

[2]R. G. Buschman and M. C. Wunderlich, Sieve-Generated sequences with translated intervals, *Canad. J. Math.*,19(1967),559 — 570;*MR* 35#2855.

[3]R. G. Buschman and M. C. Wunderlich,Sieves with generalized intervals, *Boll. Un Mat. Ital.*, (3)21(1966),362-367.

[4]Paul Erdös and Eri Jabotinsky,On sequences of integers generated by a sieving process I,II. *Nederl Akad. Wetensch. Proc.*, *Ser. A*61 = *Indag. Math.*,20(1958),115-128;*MR*21#2628.

[5]Verna Gardiner,R. Lazarus,N. Metropolis,and S. Ulam,On certain sequences of integers defined by sieves, *Math. Mag.*,29(1956),117-122; *MR* 17,711.

[6]David Hawkins and W. E. Briggs,The lucky number theorem, *Math. Mag.*,31(1957-58),81-84,277-280;*MR* 21#2629,2630.

[7]M. C. Wunderlich,Sieve generated sequences, *Canad. J. Math.*, 18 (1966),291-299;*MR* 32#5625.

[8]M. C. Wunderlich, A general class of sieve-generated sequences, *Acta Arith.*, 16 (1969-70), 41-56; *MR* 39#6852.
[9]M. C. Wunderlich and W. E. Briggs, Second and third term approximations of sieve-generated sequences, *Illinois J. Math.*, 10(1966), 694-700; *MR* 34#153.

C3. Ulam 数

Ulam 构造正整数递增序列：初始值 u_1, u_2 取任意值，而后继项仅能用一种方式表为序列前面的两不同项的和. Recáman 问了一些与 Ulam 数相关的问题，Ulam 数（$u_1 = 1, u_2 = 2$）如下：
1,2,3,4,6,8,11,13,16,18,26,28,36,38,47,48,53,57,62,69,72,77,82,87,97,99,102,106,114,126,131,138,145,148,155,175,177,180,182,189,197,206,209,219,…

(1)除开 1+2=3 外，相邻 Ulam 数的和还是 Ulam 数吗？

(2)存在无穷多个数

23,25,33,35,43,45,67,92,94,96,…

它不是两个 Ulam 数的和吗？

(3)Ulam 数有正密率吗？（此问题系 Ulam 本人所提）

(4)存在无穷多对相邻 Ulam 数对吗？如，

(1,2),(2,3),(3,4),(47,48),…

(5)在 Ulam 数序列中，存在任意大的间隔吗？

在解决问题(1)时，Frank Owens 注意到 $u_{19} + u_{20} = 62 + 69 = 131 = u_{31}$. 在解决问题(4)时，Muller 计算了 20000 项，没有找到更进一步的例子. 另一方面，这 20000 项中，有多于 60% 的两项的差恰为 2. David Zeitlin 问 $a(n)$ 和 $b(n)$ 如何？它们的定义如下：

$$u_{n+3} = u_{n+2-a(n)} + u_{n+1-b(n)} \quad (a(n) \leqslant b(n), n \geqslant 0).$$

$n=$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$a(n)=$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	5

$b(n)=$	1	1	2	2	4	4	6	3	8	5	10	6	13	10	12	6
$n=$	17	18	19	20	21	22	23	24	25	26	27	28	29	…		
$a(n)=$	2	0	1	2	3	4	0	0	0	0	9	10	4	…		
$b(n)=$	9	16	14	13	12	11	22	22	22	21	10	20	17	…		

他注意到，对于 $n=1,2,3,4,5,7,11,21$ 和 23 有 $b(n)=\varphi(n)$，因此他问使 $b(n)=\varphi(n)$ 成立的 n 是否有无穷多个？他又问，从每一整数都可表为序列不同元素之和意义上来看，Ulam 序列是否是完全的？他还问，Fibonacci 数(和 Lucas 数)总是至多不超过两个 Ulam 数的和吗？

[1]A. M. Mian and S. Chowla, On the B_2-sequence of Sidon, *Proc. Nat. Acad. Sci. India. Sect. A*, 14(1949), 3-4; *MR* 7, 243.

[2]P. Muller, M. Sc. thesis, Univ. of Buffalo, 1966.

[3] R. Queneau, Sur les suites s-additives, *J. Combinatorial Theory*, 12(1972), 31-71.

[4]Bernardo Recamán, Questions on a sequence of Ulam, *Amer. Math. Monthly*, 80(1973), 919-920.

[5]S. M. Ulam, *Problems in Modern Mathematics*, Interscience, N. Y. 1964, ix.

[6]M. C. Wunderlich, The improbable behaviour of Ulam's summation sequence, in *Computers and Number Theory*, Academic Press, 1971, 249-257.

C4. 和产生集合问题

一个集合 $\{x_i\}$ 的所有数对之和 $x_i+x_j(i\neq j)$ 构成一个新的集合$\{y_i\}$，称为$\{x_i\}$ 产生$\{y_i\}$. Leo Moser 提出了被称为"和产生集合"问题：有多少集合$\{x_i\}$ 产生同一个集合$\{y_i\}$？Selfridge, Straus 和其他人证明了，如果集合 $\{x_i\}$ 的元素个数不是 2 的幂，则产生同一集合$\{y_i\}$ 的那些集合的个数是确定的. 假定 $y_1,y_2,\cdots,y_s$ 是由 $x_1,x_2,\cdots,x_{2^k}$ 的和 $x_i+x_j(i\neq j)$ 产生的，则 $s=2^{k-1}(2^k-1)$. 那

么，存在两个以上的集合$\{x_i\}$，它产生了相同的集合$\{y_i\}$吗？如果$k = 3$，则存在三个这样的集合$\{x_i\}$，如：

$$\{\pm 1, \pm 9, \pm 15, \pm 19\}, \{\pm 2, \pm 6, \pm 12, \pm 22\},$$
$$\{\pm 3, \pm 7, \pm 13, \pm 21\},$$

且不可能有多于 3 个的集合$\{x_i\}$. 但对$k > 3$，该问题没有解决.

与此相应的问题是：一个集合$\{x_i\}$的元素的三个一组的和确定集合的问题除开下面的两种情形外已全部解决. 两种例外情形为：$\{x_i\}$的元素个数为$n = 27$或$n = 486$.

4 个不同元素的和已被 Ewell 解决.

[1]John A. Ewell, On the determination of sets by sets of sums of fixed order, *Canad. J. Math.*, 20(1968), 596 — 611.

[2]B. Gordon, A. S. Fraenkel, and E. G. Straus, On the determination of sets by the sets of sums of a certain order, *Pacific J. Math.*, 12(1962), 187-196; *MR* 27#3576.

[3]J. L. Selfridge and E. G. Straus, On the determination of numbers by their sums of a fixed order, *Pacific J. Math.*, 8(1958), 847-856; *MR* 22#4657.

C5. 堆垒链

关于n的堆垒链是序列$1 = a_0 < a_1 < \cdots < a_r = n$，它的每一项(第 0 项以后)都是前面的两个数之和(这里两数不一定不同)，如，

$$1, 1+1, 2+2, 4+2, 6+2, 8+6$$

和

$$1, 1+1, 2+2, 4+2, 4+4, 8+6$$

是长为$r = 5, n = 14$的堆垒链. 现用$l(n)$表n的堆垒链的最小长度.

现在主要的未决问题是 Scholz 猜想：

$$l(2^n - 1) \leqslant n - 1 + l(n).$$

Utz, Gioia 等人和 Knuth 已证明了$n = 2^a, 2^a + 2^b, 2^a + 2^b + 2^c, 2^a$

$+2^b+2^c+2^d$ 的情形. Knuth 和 Thurber 已用实例说明了 $1\leqslant n\leqslant 18$ 和 $n=20,24,32$ 时的情形. Brauer 引进了序列 $1=a_0<a_1<\cdots<a_r=n$，该序列的每一项都用它前一项元素作为一个被加数. 我们称 Brauer 引进的这个序列为 Brauer 链. 上面的第二个例子不是 Brauer 链，因为 4+4 那一项没有被加数 6. 使 Brauer 链最短的 n 为 Brauer 数，则 Brauer 证明了猜想对 Brauer 数 n 成立. Hansen 证明了，存在无穷多个非 Brauer 数，且如果 n 具有被称为 Hansen 链的最短链，则 Scholz 猜想仍然成立. Hansen 链是指，存在一个链的子集合 H，使得链中的每一个元素都用 H 中比该元素小的最大元素组成. 上述第二个例子便是 Hansen 链，这里 $H=\{1,2,4,8\}$. Knuth 给出的一个例子是 $n=12509$ 的 Hansen 链 1，2，4，8，16，17，32，64，128，256，512，1024，1041，2082，4164，8328，8345，12509（这里 $H=\{1,2,4,8,16,32,64,128,256,512,1024,1041,2082,4164,8328,8345\}$）. 它不是 Brauer 链（因为 32 不用 17 组成），且对于 $n=12509$，不存在这样短的 Brauer 链.

存在非 Hansen 数吗？

[1]Alfred Brauer, On addition chains, *Bull. Amer. Math. Soc.*, 45(1939), 736-739; *MR* 1, 40.

[2]Paul Erdős, Remarks on number theory III. On addition chains, *Acta Arith.*, 6(1960), 77-81.

[3]A. A. Gioia and M. V. Subbarao, The Scholz-Brauer problem in addition chains II, *Congressus Numerantiun XXII*, Proc. 8th Manitoba Conf. Numerical Math. Comp., 1978, 251-274; *MR* 80*i*: 10078; *Zbl.* 408. 10037.

[4]A. A. Gioia, M. V. Subbarao and M. Sugunamma, The Scholz-Brauer problem in addition chains, *Duke Math. J.*, 29(1962), 481-487; *MR* 25#3898.

[5]W. Hansen, Zum Scholz-Brauerschen Problem, *J. reine angew. Math.*, 202(1959), 129-136; *MR* 25#2027.

[6]A. M. Il'in, On additive number chains (Russian), *Problemy Kibernet.*,

13(1965),245-248.

[7]Donald Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Reading, Mass., 1969, 398-422.

[8] Arnold Scholz, Aufgabe 253, *Jber. Deutsch. Math.-Verein.*, II 47(1937), 41-42.

[9]K. B. Stolarsky, A lower bound for the Scholz-Brauer problem, *Canad. J. Math.*, 21(1969), 675-683; *MR* 40# 114.

[10]E. G. Straus, Addition chains of vectors, *Amer. Math. Monthly*, 71(1964), 806-808.

[11]Edward G. Thurber, The Scholz-Brauer problem on addition chains, *Pacific J. Math.*, 49(1973), 229-242; *MR* 49# 7233.

[12]Edward G. Thurber, Addition chains and solutions of $l(2n) = l(n)$ and $l(2^n - 1) = n + l(n) - 1$, *Discrete Math.*, 16(1976), 279 - 289; *MR* 55# 5570; *Zbl.* 346. 10032.

[13]W. R. Utz, A note on the Scholz-Brauer problem in addition chains, *Proc. Amer. Math. Soc.*, 4(1953), 462-463; *MR* 14, 949.

[14]C. T. Wyburn, A note on addition chains, *Proc. Amer. Math. Soc.*, 16 (1965), 1134.

C6. 不可表数

给定 n 个整数 $0 < a_1 < a_2 < \cdots < a_n$，且 $(a_1, a_2, \cdots, a_n) = 1$，如果 N 充分大，那么 $N = \sum_{i=1}^{n} a_i x_i$ 有非负整数解 x_i. 设 $G(a_1, a_2, \cdots, a_n)$ 是不存在这样解的最大 N，Sylvester 证明了 $G(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$ 且不可表示数的个数是 $(a_1 - 1)(a_2 - 1)/2$. Brauer 和其他人证明了：

$$G(a_1, a_2, \cdots, a_n) \leqslant \sum_{i=1}^{n-1} a_{i+1} d_i / d_{i+1},$$

其中 $d_i = (a_1, a_2, \cdots, a_i)$. 柯召对 $s = 3$ 的情形证明了 $G(a_1, a_2, a_3) \leqslant \frac{a_1 a_2}{(a_1, a_2)} + a_3 (a_1, a_2) - a_1 - a_2 - a_3$ 且当 $N > \frac{a_1 a_2}{(a_1, a_2)^2} -$

$\frac{a_1}{(a_1,a_2)}-\frac{a_2}{(a_1,a_2)}$时,$G(a_1,a_2,a_3)=\frac{a_1a_2}{(a_1,a_2)}+a_3(a_1,a_2)-a_1-a_2-a_3$(这里 a_1,a_2,a_3 可轮换). 陈重穆推广柯召的工作,证明了:$G(a_1,a_2,\cdots,a_n)\leqslant\sum_{i=1}^{n-1}a_{i+1}d_i/d_{i+1}-\sum_{i=1}^{n}a_i$,且当 $a_{i+1}d_i/d_{i+1}>\sum_{j=1}^{i-1}a_{j+1}d_j/d_{j+1}-\sum_{j=1}^{i}a_j(3\leqslant i\leqslant n)$时,等号成立. 陆文端和吴昌玖给出了等号成立的充要条件. 如果 $a_i(i=1,\cdots,n)$ 成算术级数,则 Roberts 和 Bateman 找到了 G 的值,并且吴昌玖给出了 G 值的一个十分简短的证明,顺便还得出了线性型不能表出的正整数的个数. Erdős 和 Graham 证明了 $G(a_1,a_2,\cdots,a_n)\leqslant 2a_{n-1}[a_n/n]-a_n$(如果 $n=2$,且 a_2 为奇,则这是可能的最好结果). 关于求 G 的较为完整的算法是尹文霖得到的,例如他证明了 $G(a_1,a_2,\cdots,a_n)=\max_{\substack{\bar{n}-ka_n\notin M_{n-1}^* \\ 0\leqslant k<K}}(d_{n-1}\bar{n}+a_n(d_{n-1}-1))$,这里 $M_{n-1}^*=\{m:m=\sum_{i=1}^{n-1}\frac{a_i}{d_{n-1}}x_i$ 且 $x_i\geqslant 0(i=1,\cdots,n)\}$,$K$ 是适合 $Ka_n\in M_{n-1}^*$ 的最小正整数. 有关 G 的更为详细的情况参见曹珍富的书《丢番图方程引论》第四章 § 3.

Erdős 和 Graham 定义 $g(n,t)=\max_{\{a_i\}}G(a_1,a_2,\cdots,a_n)$,其中最大值取遍所有的 $0<a_1<a_2<\cdots<a_n\leqslant t$,且$(a_1,a_2,\cdots,a_n)=1$. 他们的定理证明了 $g(n,t)<2t^2/n$ 且对集合$\{x,2x,\cdots,(n-1)x,x^*\}(n\geqslant 2)$,这里 $x=[t/(n-1)]$,$x^*=(n-1)[t/(n-1)]-1$,有 $g(n,t)\geqslant G(x,\cdots,x^*)\geqslant t^2/(n-1)-5t$. Lewin 对于集合$\{t/2,t-1,t\}$或$\{t-2,t-1,t\}$($t$ 为偶)和$\{(t-1)/2,t-1,t\}$(t 为奇),证明了 $g(3,t)=[(t-2)^2/2]-1$.

[1]P. T. Bateman, Remark on a recent note on linear forms, *Amer. Math. Monthly*, 65(1958), 517 − 518.

[2]E. R. Berlekamp, J. H. Conway, and R. K. Guy, *Winning Ways*, Academic Press, London, 1981, Chap. 18.

[3]Alfred Brauer, On a problem of partitions, *Amer. J. Math.*, 64(1942), 299-312.

[4]A. Brauer and B. M. Seelbinder, On a problem of partitions, II, *ibid*, 76(1954), 343-346.

[5]A. Brauer and J. E. Shockley, On a problem of Frobenius, *J. reine angew. Math.*, 211 (1962), 215-220.

[6]J. S. Byrnes, On a partition problem of Frobenius, *J. Combin. Theory Ser. A* 17(1974), 162-166; *MR* 50#234.

[7]曹珍富(Z. Cao),丢番图方程引论,哈尔滨工业大学出版社,1989.

[8]陈重穆(C. Chen),关于整系数线性型的一个定理,四川大学学报(自然科学版),1956,No. 1.

[9]P. Erdős and R. L. Graham, On a linear diophantine problem of Frobenius, *Acta Arith.*, 21(1972), 399-408.

[10]B. R. Heap and M. S. Lynn, A graph-theoretic algorithm for the solution of a linear diophantine problem of Frobenius, *Numer. Math.*, 6(1964), 346-354; *MR* 30#4689.

[11]B. R. Heap and M. S. Lynn, On a linear diophantine problem of Frobenius: An improved algorithm, *ibid*, 7(1964), 226－231; *MR* 31#1227.

[12]柯召(C. Ko),关于方程 $ax+by+cz=n$,四川大学学报(自然科学版), 1(1955), 1－4.

[13]Mordechai Lewin, On a linear diophantine problem, *Bull. London Math. Soc.*, 5(1973), 75-78; *MR* 47#3311.

[14]陆文端(W. Lu),吴昌玖,关于整系数线性型的两个问题,四川大学学报(自然科学版),2(1957),151－171.

[15]N. S. Mendelsohn, A linear diophantine equation with applications to non-negative matrices, *Ann. N. Y. Acad. Sci.*, 175(1970), 287-294.

[16]A. Nijenhuis and H. S. Wilf, Representations of integers by linear forms in non-negative integers, *J. Number Theory*, 4(1972), 98-106.

[17]J. B. Roberts, Note on linear forms, *Proc. Amer. Math. Soc.*, 7(1956), 465-469.

[18]Ö. J. Rödseth, On a linear Diophantine problem of Frobenius, *J. reine angew. math.*, 301(1978), 171-178.

[19]E. S. Selmer and Ö. Beyer, On the linear diophantine problem of Frobenius in three variables, *J. reine angew. math.*, 301(1978), 161-170.

[20]J. J. Sylvester, *Math. Quest. Educ. Times*, 41(1884), 21.

[21]Herbert S. Wilf, A circle of lights algorithm for the "money changing problem", *Amer. Math. Monthly*, 85(1978), 562-565.

[22]吴昌玖(C. Wu),关于线性型的一个结果,四川大学学报(自然科学版),1(1958),33—36.

[23]尹文霖(W. Yin),关于正整数系数线性型的最大不可表数,高等学校自然科学学报(数学,力学,天文学版),试刊,1(1964),32—38.

C7. 子集和不同的集合

元素个数为 $k+1$ 的整数集合 $\{2^i: 0 \leqslant i \leqslant k\}$,其所有 2^{k+1} 个子集和(指子集中的所有元素之和)都不同. Erdős 一直想求得正整数 $a_1 < a_2 < \cdots < a_m < 2^k$ 中的最大数 m,这些正整数的集合其所有不同的子集和都不同. 他与 Leo Moser 证明了 $k+1 \leqslant m \leqslant k + \frac{1}{2}\log k + 1$,其中对数的底为 2. Conway 和 Guy 给出一个序列: $u_0 = 0, u_1 = 1, u_{n+1} = 2u_n - u_{n-r} (n \geqslant 1)$,这里 r 是最接近 $\sqrt{2n}$ 的整数. 从此序列可导出 $k+2$ 个整数的集合 $A = \{a_i = u_{k+2} - u_{k+2-i}: 1 \leqslant i \leqslant k+2\}$. 他们猜想,集合 A 的子集和是不同的(对于 $k \leqslant 40$ 已由 Mike Guy 证得). 对于 $k \geqslant 21, u_{k+2} < 2^k$,此时 $m \geqslant k+2$(对 $k \geqslant 21$),因为一旦找到具有希望基数的集合,它的基数便能通过原来元素的 2 倍或加 1(或任意奇数)来增加. A 总有不同和的子集吗?我们猜想,它有,且大体上给出了该问题的可能达到的最好结果是 $m = k+2$. Erdős 为 $m = k + O(1)$ 的证明或反例提供了 500 美元的奖金.

[1]V. S. Bludov and V. I. Uberman, A certain sequence of additively distinct numbers (Russian), *Kibernetika* (Kiev), 10(1974), # 5, 111-115; *MR* 53# 332; *Zbl*. 291. 10043.

[2]V. S. Bludov and V. I. Uberman, On a sequence of additively differing numbers, *Dopovidi Akad. Nauk. Ukrain. SSR Ser. A*, (1974), 483-486, 572; *MR* 50 # 7007; *Zbl.* 281. 10030.

[3]J. H. Conway and R. K. Guy, Sets of natural numbers with distinct sums, *Notices Amer. Math. Soc.*, 15(1968), 345.

[4]J. H. Conway and R. K. Guy, Solution of a problem of P. Erdős, *Colloq. Math.*, 20(1969), 307.

[5]P. Erdős, Problems and results in additive number theory, *Colloque sur la Théorie des Nombres*, Bruxelles, 1955, Liege and Paris, 1956, 127-137, esp. p. 137.

[6]Hansraj Gupta, Some sequences with distinct sums, *Indian J. Pure Math.*, 5(1974), 1093-1109; *MR* 57 # 12440.

[7]B. Lindström, On a combinatorial problem in number theory, *Canad. Math. Bull.*, 8(1965), 477-490.

[8]B. Lindström, Om ett problem av Erdős for talfoljder, *Nordisk Mat. Tidskrift*, 16, 1-2(1968), 29-30, 80.

[9]Paul Smith, Problem E 2536*, *Amer. Math. Monthly*, 82(1975), 300. Solutions and comments, 83(1976), 484.

[10]V. I. Uberman, On the theory of a method of determining numbers whose sums do not coincide (Russian), *Proc. Sem. Methods Math. Simulation & Theory Elec. Circuits, Izdat Nauk Dumka* (Kiev) 1973, 76-78, 203; *MR* 51 # 7363.

[11]V. I. Uberman, Approximation of additively differing numbers (Russian), *Proc. Sem. Methods Math. Simulation & Theory Elec. Circuits, Naukova Dumka*, Kiev, 11 (1973), 221-229; *MR* 51 # 7363; *Zbl.* 309. 68048.

[12]V. I. Uberman and V. I. Šleinikov, A computer-aided investigation of the density of additive detecting number systems (Russian), *Akad. Nauk Ukrain. SSR, Fiz.-Tehn. Inst. Nizkikh Temperatur*, Kharkov, 1978; 60pp.

C8. 整数用不同对的表示

假设 m 是整数 $1 \leqslant a_1 < a_2 < \cdots < a_m \leqslant n$ 使 $a_i + a_j$ 都是不同的最大个数，已知

$$n^{1/2}(1-\varepsilon) < m \leqslant n^{1/2} + n^{1/4} + 1.$$

上界是 Lindstrom 做出，并由 Erdös 和 Turán 改进后的结果. 下界是 Singer 做出的. Erdös 和 Turán 问，$m = n^{1/2} + O(1)$ 成立吗? Erdös 为这一问题的解决提供 500 美元的奖金.

如果 $\{a_i\}$ 是一无穷序列，Erdös 和 Turán 证明 $\limsup a_k/k^2 = \infty$，且给出满足 $\liminf a_k/k^2 < \infty$ 的一个序列. 对所有 k，存在 $a_k < ck^3$ 的序列，并且 Ajtai，Komlós 和 Szemerédi 最近证明 $a_k = O(k^3)$ 是可能的. Erdös 注意到 $\sum_{i=1}^{x} a_i^{-1/2} < c(\ln x)^{1/2}$，并问是否这是可能的最好结果?

如果 $f(n)$ 是 $n = a_i + a_j$ 解的个数，那么存在满足 $\lim f(n)/\ln n = c$ 的序列吗? Erdös 和 Turán 猜想，如果 $f(n) > 0$ 对所有充分大的 n 成立，或如果 $a_k < ck^2$ 对所有 k 成立，那么 $\limsup f(n) = \infty$. Erdös 为这一猜想的解决也提供了 500 美元奖金.

Graham 和 Sloane 用两种更明显的紧缩形式重述了这一问题.

设 $v_\alpha(k)$（相应地 $v_\beta(k)$）是最小的 v，使得存在 k 个元素的整数集合 $A = \{0 = a_1 < a_2 < \cdots < a_k\}$ 满足对于 $i < j$（相应地 $i \leqslant j$），有 $a_i + a_j$ 属于 $[0, v]$，且至多一次表示 $[0, v]$ 中的元素. 与 v_β 有关的集合 A 常被称为 B_2 — 序列（与 E22 比较）.

他们给出了列在表 3 中的 v_α 和 v_β 值，且只要修改一下 Erdös—Turán 的论证就可得到界：

$$2k^2 - O(k^{3/2}) < v_\alpha(k), v_\beta(k) < 2k^2 + O(k^{36/23}).$$

表 3. $v_\alpha(k)$, $v_\beta(k)$ 的值及例集

k	$v_\alpha(k)$	A 的例	$v_\beta(k)$	A 的例
2	1	{0,1}	2	{0,1}
3	3	{0,1,2}	6	{0,1,3}
4	6	{0,1,2,4}	12	{0,1,4,6}
5	11	{0,1,2,4,7}	22	{0,1,4,9,11}
6	19	{0,1,2,4,7,12}	34	{0,1,4,10,12,17}
7	31	{0,1,2,4,8,13,18}	50	{0,1,4,10,18,23,25}
8	43	{0,1,2,4,8,14,19,24}	68	{0,1,4,9,15,22,32,34}
9	63	{0,1,2,4,8,15,24,29,34}	88	{0,1,5,12,25,27,35,41,44}
10	80	{0,1,2,4,8,15,24,29,34,46}	110	{0,1,6,10,23,26,34,41,53,55}

[1]R. C. Bose and S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helv.*, 37(1962-63), 141-147.

[2]P. Erdös and W. H. J. Fuchs, On a problem of additive number theory, *J. London Math. Soc.*, 31(1956), 67-73.

[3]P. Erdös and E. Szemerédi, The number of solutions of $m = \sum_{i=1}^{k} x_i^k$, *Proc. Symp. Pure Math. Amer. Math. Soc.*, 24(1973), 83-90.

[4]P. Erdös and P. Turán, On a problem of Sidon in additive number theory, and on some related problems, *J. London. Math. Soc.*, 16(1941), 212-215; *MR* 3, 270. Addendum, 19(1944), 208; *MR*7, 242.

[5]R. L. Graham and N. J. A. Sloane, On additive bases and harmonious graphs, *SIAM J. Alg. Discrete Math.*, 1(1980), 382-404.

[6]H. Halberstam and K. F. Roth, *Sequences*, Vol. I, Oxford Univ. Press, 1966, Chapter II.

[7] F. Krückeberg, B_2-Folgen und verwandte Zahlenfolgen, *J. reine angew. Math.*, 206(1961), 53-60.

[8] B. Lindstrom, An inequality for B_2-sequences, *J. Combin. Theory*, 6(1969), 211-212; *MR* 38#4436.

[9]J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, 43(1938), 377-385.

[10]Alfred Stöhr, Gelöste und ungelöste Fragen über Basen der naturlichen Zahlenreihe I, II, *J. reine angew. math.*, 194(1955), 40-65, *III*-140;

MR 17.713.

C9. **完全差集与纠错码**

在 C8 中提到的 Singer 的结果是以完全差集为基础的. 完全差集指存在一个模 n 剩余 $a_1, a_2, \cdots, a_{k+1}$ 的集合,使得每一模 n 非零剩余能被唯一表成 $a_i - a_j$ 的形式. 仅当 $n = k^2 + k + 1$ 时才存在完全差集,并且 Singer 证明了,只要 k 为素数幂,则这样的集合存在. Marshall Hall 已证明,许多非素数幂不能作为 k 的数值. E-vans 和 Mann 证明,当 $k < 1600$ 时,不存在这样的不是素数幂的 k. 人们猜想,除非 k 是素数幂,否则不存在完全差集.

对于一给定的有限序列,它不含有重复差,问它能被扩展形成一完全差集吗?

Dean Hickerson 欲求最大数值 r,使整数 $1 \leqslant a_1 < a_2 < \cdots < a_r \leqslant n$ 的差 $a_j - a_i (j > i)$ 中,整数 s 至多出现 $2s$ 次.

Graham 和 Sloane 仿 C8 的紧缩问题来提出差集问题. 他们定义 $v_\gamma(k)$(相应地 $v_\delta(k)$)为最小数 v,使得存在整数模 v 的集合 $A = \{0 = a_1 < a_2 < \cdots < a_k\}$,而每一个 r 至多能用一种方式表为 $r \equiv a_i + a_j \pmod{v} (i < j)$(相应地 $i \leqslant j$).

他们对 v_γ 的兴趣是其在纠错码中的应用. 如果 $A(k, 2d, w)$ 是有 w 个 1 和 $k - w$ 个 0 的二进制向量,使得任两向量至少在 $2d$ 处不同的最大个数,则(对 $d = 3$)

$$A(k, 6, w) \geqslant \binom{k}{w} / v_\gamma(k)$$

(对一般 d 的结果要用到集合,它的所有 $d - 1$ 个不同元素的和是不同的(mod v)).

他们注意到, $A(k, 2d, w)$ 已被 Erdős, Hanani, Schönheim, Stanton, Kalbfleisch 和 Mullin 在关于极值集论的文章中研究过. 设 $D(t, k, v)$ 是 v 元集合 S 的 k 元子集,使得 S 的每一个 t 元子集至多含有 k 元子集中的一个的最大个数,那么 $D(t, k, v) = A(v, 2k$

$-2t+2,k)$.

表 4 中的 v_δ 值来自 Baumer 的表 6.1，v_γ 来自 Graham 和 Sloane，他们给出了下面的界：

$$k^2-O(k)<v_\gamma(k)<k^2+O(k^{36/23}),$$

$$k^2-k+1\leqslant v_\delta(k)<k^2+O(k^{36/23}),$$

其中，后一个左边的等式只要 k 为素数幂就成立.

表 4. $v_\gamma(k)$ 和 $v_\delta(k)$ 的值及例集

k	$v_\gamma(k)$	A 的例	$v_\delta(k)$	A 的例
2	2	{0,1}	3	{0,1}
3	3	{0,1,2}	7	{0,1,3}
4	6	{0,1,2,4}	13	{0,1,3,9}
5	11	{0,1,2,4,7}	21	{0,1,4,14,16}
6	19	{0,1,2,4,7,12}	31	{0,1,3,8,12,18}
7	28	{0,1,2,4,8,15,20}	48	{0,1,3,15,20,38,42}
8	40	{0,1,5,7,9,20,23,35}	57	{0,1,3,13,32,36,43,52}
9	56	{0,1,2,4,7,13,24,32,42}	73	{0,1,3,7,15,31,36,54,63}
10	72	{0,1,2,4,7,13,23,31,39,59}	91	{0,1,3,9,27,49,56,61,77,81}

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture notes in Math. 182, Springer-Verlag, New York, 1971.

[2] M. R. Best, A. E. Brouwer, F. J. MacWilliams A. M. Odlyzko and N. J. A. Sloane, Bounds for binary codes of length less than 25, *IEEE Trans. Information Theory*, IT-24(1978), 81-93.

[3] P. Erdős and H. Hanani, On a limit theorem in combinatorical analysis, *Publ. Math. Debrecen*, 10(1963), 10-13.

[4] T. A. Evans and H. Mann, On simple difference sets, *Sankhya*, 11(1951), 357-364; *MR* 13, 899.

[5] R. L. Graham and N. J. A. Sloane, Lower bounds for constant weight codes, *IEEE Trans. Information Theory*, IT-26(1980).

[6] J. I. Hall, A. J. E. M. Jensen, A. W. J. Kolen and J. H. van Lint, Equidis-

tant codes with distance 12, *Discrete math.*, 17(1977), 71-83.
[7]M. Hall, Cyclic projective planes, *Duke Math. J.*, 14(1947), 1079-1090; *MR* 9, 370.
[8]D. McCarthy, R. C. Mullin, P. J. Schellenberg, R. G. Stanton, and S. A. Vanstone, On approximations to a projective plane of order 6, *Ars Combinatoria*, 2(1976), 111-168.
[9]F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
[10]J. Schönheim, On maximal systems of k-tuples, *Stud. Sci. Math. Hungar*, 1(1966), 363-368.
[11]R. G. Stanton, J. G. Kalbfleisch and R. C. Mullin, Covering and packing designs, in *Proc. 2nd Conf. Combin. Math. and Appl.*, Chapel Hill, 1970, 428-450.

C10. 和不同的三个元素子集

Bose 和 Chowla 研究当三个不同元素的子集都有不同的和时，对 C9 的问题获得了类似的结果. 如果 m_3 是满足 $1 \leqslant a_1 < a_2 < \cdots < a_{m_3} \leqslant n$，使得 $a_i + a_j + a_k$ 都是不相同的 a_i 的最大个数，则他们证明了 $m_3 \geqslant n^{1/3}(1 + o(1))$，且他们问是否 $m_3 \geqslant (1 + \varepsilon)n^{1/3}$？

Lindström 已证明，如果 m_4 是 $\leqslant n$ 的整数中 4 个不相同元素的集合有不同和的最大个数，那么 $m_4 < (8n)^{1/4} + O(n^{1/8})$.

[1]S. C. Bose and S. Chowla, *Report Inst. Theory of Numbers*, Univ. of Colorado, Boulder, 1959.
[2]B. Lindström, A remark on B_4-sequences, *J. Combin. Theory*, 7(1969), 276-277.

C11. *h*-基

覆盖问题是 Rohrbach 提出的. 此问题与 C8 中的紧缩问题是孪生的. 如果集 A 的每一个不大于 n 的非负整数能被表成至多 h 个 A 中元素的和(不一定必须不相同)，则称 A 是阶为 h 的堆垒基

或 h-基(对于 n). 如果 h 是使 A 具有这类特性的最小数,那么 h 被称为 A 的确阶. 如果 $k_h(n)$ 是对于 n 的 h-基中元素的最小个数,则 Rohrbach 证明了, $k_h(n) < hn^{1/h}$ 和 $(1/2)k_2^2(1-0.0016) > n$. 接着,Leo Moser, Riddell 和 Klotz 改进了他的结果,先是用 0.0194 代替 0.0016,然后是 0.0269,再往后是 0.0369,他们还证明了,对于 $h \geqslant 3, 0 < \varepsilon < 1$,且对充分大 n,有

$$\frac{k_h}{h!}\left\{1 - \frac{(1-\varepsilon)\cos\pi/h}{2+\cos\pi/h}\right\} > n.$$

设 $n(h,k)$ 是使 k 元的 h-基存在的最大整数,那么,确定 $n(h,k)$ 的问题经常出现,如同邮票或钱币问题一样,详细的情况及广泛的文献请见 Alter 和 Barnett 的论文.

Rohrbach 证明了 $n(2,k) \geqslant k^2/4$ 并且猜测 $n(2,k)/k^2$ 随 $k \to \infty$ 而趋于 1/4. 但是,这已被 Hammerer 和 Hofmeister 证明是错的. 关于 $n(2,k)$ 的具有 $k_2(n)$ 个元素的基被称为极值的,如果 2-基(对于 n) 的元素不超过 $n/2$,则此基被称为是约化的. Rohrbach 的基是关于 $n/4$ 对称的(因此是约化的). 例如,$n(2,10)=46$,但是对于 46 的仅有的极值基:

1,2,"3 或 5",7,11,15,19,21,22,24

是约化的. 读文献时需要加点小心:这一结果很可能在文章中被写成 $n(2,11)=46$,在那里每一非负整数恰能被表达成基的 h 个元素(不一定不相同)的和. 这与零面额邮票或钱币问题的结论相对应. 如果某极值基是约化的,那么它必定是对称的吗?

Stöhr 和几位稍后的一些作者证明了:

$$n(h,2) = [(h^2+6h+1)/4],$$

且 Hofmeister 证明了,对于 $h \geqslant 34$,

$$\frac{4}{81}h^3 + \frac{2}{3}h^2 + \frac{66}{27}h \leqslant n(h,3) \leqslant \frac{4}{81}h^3 + \frac{2}{3}h^2 + \frac{71}{27}h - \frac{1}{81}.$$

Stöhr 等人认为,对充分大 h,$n(h,k)$ 由 h 中的 k 次多项式的有限集合给定,特别地,对 $k=3$ 和 $h \geqslant 20$,

$$n(h,3) = (4h^3 + 54h^2 + (204 + 3c_r)h + d_r)/81,$$

其中 c_r, d_r 在 $h \equiv r \pmod 9$ 时由下式给定：

$r =$	-4	-3	-2	-1	0	1	2	3	4
$c_r =$	0	1	3	0	-2	0	3	1	0
$d_r =$	46	-81	-1	-170	0	62	-26	0	-154

对于固定的 $k > 2$ 和大 h，Hofmeister 给出界：

$$2^{[k/4]}\left(\frac{4}{3}\right)^{[k-4[k/4]]}\left(\frac{h}{k}\right)^k + O(h^{k-1}) \leqslant n(h,k) \leqslant \frac{h^k}{k!} + O(h^{k-1}).$$

Graham 和 Sloane（请参见 C8，C9）定义 $n_\alpha(k)$（相应地 $n_\beta(k)$）为使得存在 k 元整数集合 $A = \{0 = a_1 < a_2 < \cdots < a_k\}$，在 $[1,n]$ 中的 r 都至少能用一种方式写成 $r = a_i + a_j, i < j$（相应地 $i \leqslant j$）的最大数 n. 因此，他们的 $n_\beta(k)$ 可写为 $n(2, k-1)$（注意上面提到的“零条件”），且他们的 $n_\alpha(k)$ 与具有不同面值的两张邮票问题相对应，且包含零面值. 他们在表 5 中给出了 n_α 和 n_β 的值. 界

表 5　n_α 和 n_β 的值及例集

k	$n_\alpha(k)$	A 的例	$n_\beta(k)$	A 的例
2	1	{0,1}	2	{0,1}
3	3	{0,1,2}	4	{0,1,2}
4	6	{0,1,2,4}	8	{0,1,3,4}
5	9	{0,1,2,3,6}	12	{0,1,3,5,6}
6	13	{0,1,2,3,6,10}	16	{0,1,3,5,7,8}
7	17	{0,1,2,3,4,8,13}	20	{0,1,2,5,8,9,10}
8	22	{0,1,2,3,4,8,13,18}	26	{0,1,2,5,8,11,12,13}
9	27	{0,1,2,3,4,5,10,16,22}	32	{0,1,2,5,8,11,14,15,16}
10	33	{0,1,2,3,4,5,10,16,22,28}	40	{0,1,3,4,9,11,16,17,19,20}
11	40	{0,1,2,4,5,6,10,13,20,27,34}	46	{0,1,2,3,7,11,15,19,21,22,24}
12	47	{0,1,2,3,6,10,14,18,21,22,23,24}	54	{0,1,2,3,7,11,15,19,23,25,26,28}
13	56	{0,1,2,4,6,7,12,14,17,21,30,39,48}	64	{0,1,3,4,9,11,16,21,23,28,29,31,32}
14	65	{0,1,2,4,6,7,12,14,17,21,30,39,48,57}	72	{0,1,3,4,9,11,16,20,25,27,32,33,35,36}

$$\frac{5}{18}(k-1)^2 < n_\alpha(k), n_\beta(k) < 0.4802k^2 + O(k)$$

实际上要归功于 Hämmerer 和 Hofmeister 及 Klotz 做的工作.

[1]R. Alter and J. A. Barnett, Remarks on the postage stamp problem with applications to computers, *Congressus Numerantiun XIX*, Proc. 8th S. E. Conf. Combin, Graph Theory, Comput., Utilitas Math., 1977, 43-59; *MR* 57#12246.

[2]R. Alter and J. A. Barnett, A postage stamp problem, *Amer. Math Monthly*, 87(1980), 206-210.

[3]N. Hammerer and G. Hofmeister, Zu einer Vermutung von Rohrbach, *J. reine angew. Math.*, 286/287 (1976), 239-247; *MR* 54#10181.

[4] E. Härtter, Basen für Gitterpunktmengen, *J. reine angew. Math.*, 202(1959), 153-170; *MR 22A*#31.

[5]R. L. Heimer and H. Langenbach, The stamp problem, *J. Recreational Math.*, 7(1974), 235-250.

[6]G. Hofmeister, Asymptotische Abschätzungen für dreielementige Extremalbasen in natürlichen Zahlen, *J. reine angew. Math.*;232(1968), 77-101; *MR* 38#1068.

[7]G. Hofmeister, Endliche additive Zahlentheorie, Kapitel I, Das Reichweitenproblem, Joh. Guttenberg-Univ. Mainz, 1976.

[8]G. Hofmeister and H. Schell, Reichweiten von Mengen naturlicher Zahlen I, *Norske Vid. Selsk. Skr.* (Trondheim) 1970#10, 5pp; *MR* 44#1642.

[9]W. Klotz, Eine obere Schranke für die Reichweite einer Extremalbasis zweiter Ordnung, *J. reine angew. Math.*, 238(1969), 161-168 (and see 194-220); *MR*40#117, 116

[10] W. F. Lunnon A postage stamp problem, *Comput. J.*, 12(1969), 377-380; *MR* 40#6745.

[11]L. Moser, On the representation of 1, 2, …, n by sums, *Acta Arith.*, 6(1960), 11-13; *MR 23A*#133.

[12]L. Moser, J. R. Pounder and J. Riddell, On the cardinality of h-bases for n, *J. London Math. Soc.*, 44(1969), 397-407; *MR* 39#162.

[13]L. Moser and J. Riddell, On additive h-bases for n, *Colloq. Math.*, 9(1962), 287-290; *MR* 26#1295.

[14]Arnulf Mrose, Untere Schranken für die Reichweiten von Extremalbasen fester Ordnung, *Abh. Math. Sem. Univ. Hamburg*, 48(1979), 118-124; *MR* 80g:10058.

[15]M. B. Nathanson, Additive h-bases for lattice points, 2nd Internat. Conf. Combin. Math., *Annals N. Y. Acad. Sci.*, 319(1979), 413-414; *MR* 81e:10041

[16]J. Riddell, On bases for sets of integers, Master's thesis, Univ. of Alberta. 1960.

[17]J. Riddell and C. Chan, Some extremal 2-bases, *Math. Comp.*, 32(1978), 630-634; *MR* 57#16244; *Zbl.* 388.10032.

[18]H. Rohrbach, Ein Beitrag zur additiven Zahlentheorie, *Math. Z.*, 42(1937), 1-30; *Zbl.* 15, 200.

[19]H. Rohrbach, Anwendung eines Satzes der additiven Zahlentheorie auf eine graphen-theoretische Frage, *Math. Z.*, 42(1937), 538-542.

[20]R. G. Stanton, J. A. Bate and R. C. Mullin, Some tables for the postage stamp problem, *Congressus Numerantium XII*, Proc. 4th Manitoba Conf. Numer. Math. Winnipeg 1974, 351-356; MR 51#7887.

C12. 模覆盖问题、和谐图

Graham 和 Sloane 定义 $n_\gamma(k)$(相应地 $n_\delta(k)$) 为一个最大数 n,对此 n,存在模 n 剩余类的子集 $A=\{0=a_1<a_2<\cdots<a_k\}$,满足:每个 r 至少能用一种方式表为 $r\equiv a_i+a_j \pmod n$,且 $i<j$(相应为 $i\leqslant j$).

他们给出了表 6 中的数值,且得到界为:

$$\frac{5}{18}(k-1)^2<n_\gamma(k), n_\delta(k)<\frac{1}{2}k^2+O(k).$$

表 6　n_γ 和 n_σ 的值及例集

k	$n_\gamma(k)$	A 的例	$n_\delta(k)$	A 的例
2	1		3	{0,1}
3	3	{0,1,2}	5	{0,1,2}
4	6	{0,1,2,4}	9	{0,1,3,4}
5	9	{0,1,2,4,7}	13	{0,1,2,6,9}
6	13	{0,1,2,3,6,10}	19	{0,1,3,12,14,15}
7	17	{0,1,2,3,4,8,13}	21	{0,1,2,3,4,10,15}
8	24	{0,1,2,4,8,13,18,22}	30	{0,1,3,9,11,12,16,26}
9	30	{0,1,2,4,10,15,17,22,28}	35	{0,1,2,7,8,11,26,29,30}
10	36	{0,1,2,3,6,12,19,20,27,33}		

他们称有 v 个顶点和 e 条边($e \geqslant v$) 的联接图为和谐的，如果用不同标号 $l(x)$ 去标顶点 x，使得当边 xy 用 $l(x)+l(y)$ 来标时，边的标号形成一个完全剩余系(mod e). 树(满足 $e=v-1$)也被称为和谐的，如果仅有一个顶点标号被重复且边标号形成一个完全剩余系(mod $v-1$). 与前一个问题的关联是：$n_\gamma(v)$ 恰是有 v 个顶点的任意和谐图中边的最大个数. 例如，从表 6 中，我们注意到：$n_\gamma(5)=9$，有集合{0,1,2,4,7}，因此 9 条边中的最大值能出现在

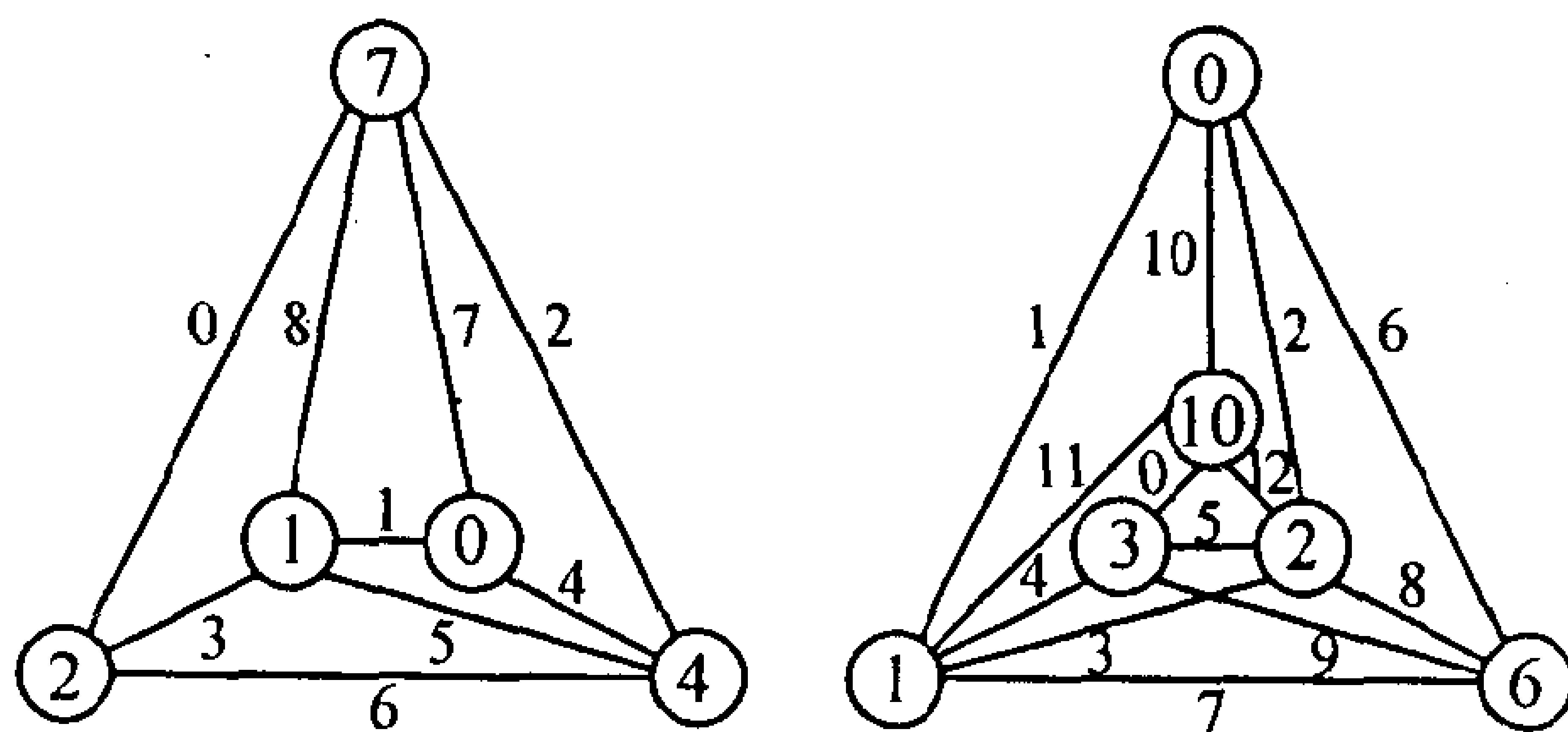


图 6　模 9 与模 13 的和谐图

有 5 个顶点的和谐图中(见图 6(a)). Graham 和 Sloane 把和谐图和优美图进行了比较和对照. 优美图在图论中已被讨论. 如果一个

图的顶点标号是选自[0, e]且边标号由 $|l(x)-l(y)|$ 来计算，则此图是优美的. 后者全都是不同的（也就是说，从[1,e]中取值).

人们猜想，树既是和谐的，又是优美的. 但是，这是一个未解决问题. 如果 n 为奇，则圈 c_n 是和谐的；如果 $n\equiv 0$ 或 $3 \pmod 4$，则圈 c_n 是优美的；友图或风车仅当 $n\not\equiv 2 \pmod 4$ 时是和谐，仅当 $n\equiv 0$ 或 $1 \pmod 4$ 是优美的；扇和轮既是和谐的也是优美的. 但对于立方体不是如此，对八面体也一样.

C13. 最大无和集

如果 $a_1,a_2,\cdots,a_n$ 是任意 n 个不同的自然数，则总能找到最大数 l 使它们中的 l 个 $a_{i_1},\cdots,a_{i_l}$ 满足 $a_{i_j}+a_{i_k}\neq a_m(1\leqslant j<k\leqslant l, 1\leqslant m\leqslant n)$，这里 l 记为 $l(n)$（可设 $j\neq k$，否则集合 $\{a_i=2^i|1\leqslant i\leqslant n\}$ 将推出 $l(n)=0$）. Klarner 证明了 $l(n)>c\ln n$. 另一方面，集合 $\{2^i+0,\pm 1|1<i\leqslant s+1\}$ 推出 $l(3s)<s+3$，因此，$l(n)<\frac{1}{3}n+3$. Selfridge 用集合 $\{(3m+t)2^{m-i}|-i<t<i,1\leqslant i\leqslant m\}$ 推广了这一结果，并证明了 $l(m^2)<2m$. Choi 用筛法已进一步改进此结果为 $l(n)\ll n^{0.4+\epsilon}$.

此问题能被一般化：对于每一 l，是否存在 $n_o=n_o(l)$，使得如果 $n>n_o$ 且 $a_1,a_2,\cdots,a_n$ 是某群的任意 n 个元满足任两个之积 $a_{i_1}a_{i_2}\neq e$，e 是群的单位元（这里 i_1,i_2 可能相等，因此不存在 1 阶或 2 阶的 a_i），那么存在 l 个 a_i，使得 $a_{i_j}a_{i_k}\neq a_m, 1\leqslant j<k\leqslant l, 1\leqslant m\leqslant n$？对 $l=3$ 此问题也没有得到解决.

[1]S. L. G. Choi, On sequences not containing a large sum-free subsequence, *Proc. Amer. Math. Soc.*, 41(1973), 415-418; *MR* 48#3910.

[2]S. L. G. Choi, On a combinatorial problem in number theory, *Proc. London Math. Soc.*, (3)23(1971), 629-642; *MR* 45#1867.

[3]P. H. Diananda and H.-P. Yap, Maximal sum-free sets of elements of finite groups, *Proc. Japan Acad.*, 45(1969), 1-5; *MR* 39#6968.

[4]Leo Moser, Advanced problem 4317, *Amer. Math. Monthly*, 55(1948), 586; solution Robert Steinberg, 57(1950), 345.

[5]Anne Penfold Street, A maximal sum-free set in A_5, *Utilitas Math.*, 5(1974), 85-91; *MR* 49#7156.

[6]Anne Penfold Street, Maximal sum-free sets in abelian groups of order divisible by three, *Bull. Austral. Math. Soc.*, 6(1972), 439-441; *MR* 46#5484. Corrigenda, 7(1972), 317-318; *MR* 47#5147.

[7]P. Varnavides, On certain sets of positive density, *J. London Math. Soc.*, 34(1959), 358-560; *MR* 21#5595.

[8]H. P. Yap, Maximal sum-free sets in finite abelian groups, *Bull. Austral. Math. Soc.*, 4(1971), 217-223; *MR* 43#2081 [and see *ibid*, 5(1971), 43-54; *MR* 45#3574; *Nanta Math.*, 2(1968), 68 — 71; *MR* 38#3345; *Canad. J. Math.*, 22(1970), 1185 — 1195; *MR* 42#1897; *J. Number Theory*, 5(1973), 293-300; *MR* 48#11356].

C14. 最大无和为零的集合

Erdös 和 Heilbronn 欲求不同剩余类(mod m) 的最大数 $k = k(m)$，以致于不存在和为零的子集. 例如，集合 1，−2，3，4，5，6 表明 $k(20) \geqslant 6$，且事实上等号成立. 该例子的模式表明

$$k \geqslant [(-1 + \sqrt{8m+9})/2] \qquad (m \geqslant 5).$$

等式在 $5 \leqslant m \leqslant 24$ 成立. 可是，Selfridge 注意到，如果 m 具有形式 $2(l^2 + l + 1)$，那么集合

$$1, 2, \cdots, l-1, l, \frac{1}{2}m, \frac{1}{2}m + 1, \cdots, \frac{1}{2}m + l$$

推出

$$k \geqslant 2l + 1 = \sqrt{2m-3}.$$

实际上，他猜想，对任意偶数 m，此集合或 l 被删去的集合总能给出最好的结果，例如，$k(42) \geqslant 9$.

另一方面，如果 p 是下列区间内的素数

$$\frac{1}{2}k(k+1) < p < \frac{1}{2}(k+1)(k+2),$$

他猜想 $k(p)=k$，其中集合可能仅为

$$1,2,\cdots,k.$$

$k(43)=8$ 的情形已被 Clement Lam 证得. 因此，k 不是 m 的单调函数. 目前，仅知的比 $k\geqslant[\sqrt{2m-3}]$ 好的结果是 $k(25)\geqslant\sqrt{50-1}=7$. 后者的证明借助于集 1,6,11,16,21,5,10. 如果 $m=25l(l+1)/2$ 为奇，那么，极可能用集合 $1,-2,3,4,\cdots$ 进行改进. 但是，如果 $m=25l(l+1)/2$ 为偶，那么已给出的构造总是较好的.

$k=[(-1+\sqrt{8m+9})/2]$ 对于无穷多个 m 成立吗？

对于上述的 m 值，存在一个实现集，其中不存在与 m 互素的元素吗？例如，$m=12$：{3,4,6,10} 或 {4,6,9,10}. 存在一个 m 值，使得所有的实现集都具有此种类型吗？

Erdös 和 Heilbronn 证明了，如果 $a_1,a_2,\cdots,a_k$（这里 $k\geqslant 3(6p)^{1/2}$）是不同剩余(mod p)，p 为素数，那么每一剩余(mod p)都能写成 $\sum_{i=1}^{k}\varepsilon_i a_i$，$\varepsilon_i=0$ 或 1. 他们猜想，对 $k>2\sqrt{p}$ 同样成立，且这是可能达到的最好结果. Olsen 证明了此猜想. 他们进一步猜想，形如 a_i+a_j 的不同剩余(mod p)的个数至少为 $2k-3$，其中 $1\leqslant i\leqslant j\leqslant k$；此问题仍未获解决.

[1]P. Erdös, Some problems in number theory, in *Computers in Number Theory*, Academic Press, London and New York, 1971, 405-413.

[2]P. Erdös and H. Heibronn, On the addition of residue classes mod p, *Acta Arith.*, 9 (1969), 149-159.

[3]Henry B. Mann and John E. Olsen, Sums of sets in the clementary abelian group of type (p,p), *J. Combin. Theory*, 2(1967), 275-284.

[4]John E. Olsen, An addition theorem, modulo p, *J. Combin. Theory*, 5(1968), 45-52.

[5]John E. Olsen, An addition theorem for the elementary abelian group, *J. Combin. Theory*, 5(1968), 53-58.

[6]C. Ryavec, The addition of residue classes modulo n, *Pacific J. Math.*,

26(1968),367-373.
[7]E. Szemeredi, On a conjecture of Erdős and Heilbronn, *Acta Arith.*, 17(1970-71),227-229.

C15. 非平均集

Erdős 和 Straus 定义整数集合 $A=\{0\leqslant a_1<a_2<\cdots<a_n\leqslant x\}$ 为$[0,x]$上的非平均集，如果在 A 中，没有 a_i 是 A 的多于一个元素的子集的算术平均. 用 $f(x)$ 表这样的集合中元素的最大个数，用 $g(x)$ 表整数集合$[0,x]$的子集 B 中的元素的最大个数，这里 B 满足 B 的任两个不同子集有不同的算术平均，并且用 $h(x)$ 表对应的最大值，这里 B 的子集有不同的元素个数. Abbott 和 Erdős－Strans 利用 Szemerédi 结果(看 E7)证明了：

$$\frac{1}{10}\log x-O(1)<\log f(x)<\frac{2}{3}\log x+O(1),$$

$$\frac{1}{2}\log x-1<g(x)<\log x+O(\ln\ln x),$$

$$\sqrt{\log x}-1+O(1/\sqrt{\ln x})<\log h(x)<2\log\ln x+O(1),$$

并且猜想，$f(x)=\exp(c\sqrt{\ln x})=o(x^{\epsilon})$ 且 $h(x)=(1+o(1))\log x$. ($\log x=(\ln x)/\ln 2$)是以 2 为底的对数).

Erdős 起初欲求$[0,x]$中整数的最大个数 $k(x)$，此集合中，没有一元素能除尽任何其他元素的和. 这样的非除尽集合显然是非平均的. 因此，$k(x)\leqslant f(x)$. Straus 证明，$k(x)\geqslant\max\{f(x/f(x)),f(\sqrt{x})\}$.

Abbott 最近已证明，如果 $l(n)$ 是最大的 m，它使得任给 n 个整数的集合包含一 m 个元素的非平均集，那么 $l(n)<n^{1/13-\epsilon}$.

[1]H. L. Abbott, On a conjecture of Erdős and Straus on non-averaging sets of integers, *Congressus Numerantium XV*, *Proc. 5th Brit. Combin. Conf. Aberdeen*, 1975, 1-4.
[2]H. L. Abbott, Extremal problems on non-averaging and non-dividing

sets, *Pacific J. Math.*, 91(1980), 1-12.

[3] P. Erdős and E. G. Straus, Non-averaging sets II, in *Combinatorial Theory and its Applications II*, Colloq. Math. Soc. János Bolyai 4, North-Holland, 1970, 405-411.

[4] E. G. Straus, Non-averaging Sets, *Proc. Symp. Pure Math.*, 19 Amer. Math. Soc. Providence 1971, 215-222.

C16. 最小覆盖问题

设 $\{a_i\}$ 是 n 个不同整数 $1 \leqslant a_i \leqslant 2n$ 的任意集合，$\{b_j\}$ 是补集 $1 \leqslant b_j \leqslant 2n$，且 $b_j \neq a_i$. M_k 是 $a_i - b_j = k(-2n < k < 2n)$ 的解的个数且 $M = \min \max_k M_k$，其中最小值取遍序列 $\{a_i\}$. Erdős 证明了 $M > n/4$；Scherk 改进到 $M > (1 - 2^{-1/2})n$，Swierczkowski 改进到 $M > (4 - \sqrt{6})n/5$. Leo Moser 获得进一步地改进：$M > \sqrt{2}(n-1)/4$ 和 $M > \sqrt{4 - \sqrt{15}}(n-1)$. 另一方面，Motzkin 等人得到一个例子表明 $M < 2n/5$，与 Erdős 的猜想 $M = n/2$ 相反. 存在一个数 c 使 $M \sim cn$?

Leo Moser 提出一个对应问题，这里 $\{a_i\}$ 的元素个数不是 n 而是 k，$k = [\alpha n]$ 对某些实数 α 成立 $(0 < \alpha < 1)$.

[1] P. Erdős, Some remarks on number theory (Hebrew, English summary), *Riveon Lematematika*, 9(1955), 45-48; *MR* 17, 460.

[2] L. Moser, On the minimum overlap problem of Erdős, *Acta Arith.*, 5(1959), 117-119; *MR* 21#5594.

[3] T. S. Motzkin, K. E. Ralston and J. L. Selfridge, Minimum overlappings under translation, *Bull. Amer. Math. Soc.*, 62(1956), 558.

[4] S. Swierczkowski, On the intersection of a linear set with the translation of its complement, *Colloq. Math.*, 5(1958), 185-197; *MR* 21#1955.

C17. 独立的正整数集合

Selfridge 称正整数 $a_1 < a_2 < \cdots < a_k$ 的集合为独立的，如果

$\sum c_ia_i=0$(其中 c_i 是不全为 0 的整数)推出至少有一个 $c_i<-1$. 用抽屉原则很容易证明,如果 k 个正整数是独立的,那么 a_1 至少为 2^{k-1}. 他为下面的问题的解决提供 10 美元的奖金:k 个独立整数 $a_i=2^k-2^{k-i}(1\leqslant i\leqslant k)$ 的集合是仅有的其最大元素不超过 2^k 的集合吗?如果 $a_1=2^{k-1}$,则它是仅有的这样的集合.

称一无穷整数序列 $\{a_i\}$ 为弱独立的,如果任意关系式 $\sum\epsilon_ia_i=0,\epsilon_i=0$ 或 ±1 且 $\epsilon_i=0$ 除了有限次外,均推出 $\epsilon_i=0$ 对所有 i 成立. 如果上述序列对 $\epsilon_i=0,\pm1$,或 ±2 同样成立,则称为强独立的. Richard Hall 问:是否每一弱独立序列都是强独立序列的有限的并.

[1] J. L. Selfridge, Problem 123, *Pi Mu Epsilon J.*, 3(1959-64), 118, 413-414.

C18. 平方和

Paul Turán 欲知正整数 n 能被表成 4 个两两互素平方数的和,即 $n=x_1^2+x_2^2+x_3^2+x_4^2,(x_i,x_j)=1(1\leqslant i<j\leqslant4)$ 的特性. 如 $8|n$,则 n 不能这样来表示,且 George Turán 已证明,$n\equiv5\pmod 6$ 也不能这样表示.

另一方面,Paul Turán 猜想,所有正整数都能表成至多 5 个两两互素平方数的和. 所有充分大整数都能表成恰好 5 个两两互素的平方数的和吗?

I. Chowla 猜想,每一正整数是集合 $\{(p^2-1)/24|p$ 为素数,$p\geqslant5\}$ 中至多 4 个元素的和. 需要 4 个这样的加数的最小数是 33.

把这些问题与 Wright 的结果比较. 例如,Wright 证明了,如果 $\lambda_1,\cdots,\lambda_4$ 是给定的实数且 $\lambda_1+\cdots+\lambda_4=1$,则每一个有充分大奇因子的 n 能表成 $n=m_1^2+\cdots+m_4^2$,且 $|m_i^2-\lambda_in|=o(n)$. 他对 5 或更多个平方数及对 3 个平方数也有类似的结果(当然,对后一种情形,假定 n 不是形如 $4^a(8l+7)$).

Bohman, Fröberg 和 Riesel 证明了,有 31 个数不能表成不同平方数的和,且所有比 188 大的数都能表成至多 5 个不同平方数的和. 仅有 124 和 188 需要 6 个不同的平方数.

[1]Jan Bohman, Carl-Erik Fröberg and Hans Riese, Partitions in squares, *BIT*, 19(1979), 297-301; *MR* 80 k: 10043.

[2]E. M. Wright, The representation of a number as a sum of five or more squares, *Quart. J. Math. (Oxford)*, 4(1933), 37-51 and 228-232.

[3]E. M. Wright, The representation of a number as a sum of four 'almost proportional' squares, *ibid*, 7(1936), 230-240.

[4]E. M. Wright, Representation of a number as a sum of three or four squares, *Proc. London Math. Soc.*, (2)42(1937), 481-500.

D 丢番图方程

“这门学科可简要地这样来描述，它主要是讨论整系数多项式方程 $f(x_1,x_2,\cdots,x_n)=0$ 的有理解或整数解.众所周知，数个世纪以来，没有哪一个专题象这样吸引了如此众多的专业和业余的数学家的注意.也没有哪一个专题产生了象这样多的论文.”

上述这段话引自 Mordell 著《丢番图方程》(Diophantine Equations, Academic Press, London, 1969)一书的前言，它表明，这一节将比其他任何地方都令我们激动.如果你对这一专题感兴趣，还请参考柯召和孙琦著《谈谈不定方程》(上海教育出版社, 1980)以及曹珍富著《丢番图方程引论》(哈尔滨工业大学出版社, 1989).这些书都较全面论述了已知的、大量的未解决问题与结果，而且可读性强.此外，与二次域类数、椭圆曲线以及有限域等有关的丢番图问题本章没有论及.

D1. 等幂和、Euler 猜想

Euler 曾经写道：“对于许多几何学家来说，似乎 Fermat 大定理是可以推广的，就象不存在两个立方数，其和或差也为立方数的问题一样.找到三个 4 次方数，其和仍是 4 次方数是肯定不可能的(要使其和为 4 次方数，那么至少需要四个 4 次方数，尽管到目前为止尚没有人能找出这样的 4 次方数).同样地，找到四个 5 次幂其和仍为 5 次幂似乎也是不可能的.对于更高次幂也存在类似的情况.”

Euler 提出的这些问题在很长时间内没有取得任何进展.直到 1911 年，R. Norrie 才找到了四个 4 次方数的一个例子：

$$30^4 + 120^4 + 272^4 + 315^4 = 353^4.$$

50 年后,Lander 和 Parkin 给出了 Euler 一般猜想的一个反例:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

对于 $a^4 + b^4 + c^4 = d^4$ 的情形(这是 Euler 猜想的主要部分),已知 $d < 220000$ 时没有非平凡的整数解. Guy 说,甚至 $a^4 + b^4 + c^4 = d^2$ 是否有非平凡的整数解也未解决. 实际上,容易给出 $a^4 + b^4 + c^4 = d^2$ 的无穷多组非平凡的整数解,例如郑格于得到(见[8]) $a = 2st(s^2 + t^2)u^2, b = 2st(s^2 - t^2)u^2, c = (s^4 - t^4)u^2, d = (16s^4t^4 + (s^4 - t^4)^2)u^4$. 1988 年 2 月,在日本京都大学主办的"丢番图问题"国际会议上,美国 Noam D. Elkies 利用椭圆曲线给出了方程 $a^4 + b^4 + c^4 = d^4$ 的无穷多组正整数解,例如 $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$,Roger Frye 找到最小的解是

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

这是丢番图方程中的一个重要成就,但给出 $a^4 + b^4 + c^4 = d^4$ 或 $a^4 + b^4 + c^4 = d^2$ 的全部整数解仍是十分困难的.

Simcha Brudno 提出了下列问题:方程 $a^5 + b^5 + c^5 + d^5 = e^5$ 有参数解吗(当 $e \leqslant 765$ 时有一个解)? Euler 猜想有更高次幂的反例吗? Selfridge 等曾算出 $1141^6 = 1077^6 + 702^6 + 474^6 + 402^6 + 234^6 + 74^6, 102^7 = 90^7 + 85^7 + 83^7 + 64^7 + 58^7 + 53^7 + 35^7 + 12^7$. 对于方程 $\sum_{i=1}^{m} a_i^s = b^s (s \geqslant 3)$,当 $1 < m < s$ 时,除开 $s = 4,5$ 外是否有非平凡的整数解?曹珍富猜想它没有非平凡的整数解. 对 $1 < m = s$ 时,它极有可能存在非平凡整数解. 但至今还没有找到 $m = s = 7$ 的解.

从平凡解$(t,1,t,1)$产生方程 $a^4 + b^4 = c^4 + d^4$ 的参数解的方法是众所周知的. 这种方法可以用来产生所有已知的解,并且它将仅产生参数的次数为 $6n + 1$ 型的解. Guy 在他的书(D1)中指出,"为了回答 Brudno 的问题, $6n + 1$ 不必是素数. 尽管 25 次没出现,49 次却出现了". Choudhry 于最近找到了 25 次的含两个参数

的解.

Swinnerton-Dyer 有另一种从旧解中产生新解的方法，并且与对称性一起能证明这两种方法产生了所有的非奇异解，即产生了所有的非奇异曲线对应的解. 此外，从他能给出找到给定次数的所有非奇异解的有限过程的意义上来说，他的方法是构造性的. 所有非奇异解次数均为奇，且所有充分大的奇次都出现. 不运气地，奇异解也存在. Swinnerton-Dyer 有产生奇异解的方法，但是，没有理由认为他的方法产生全部的奇异解. 把这些解全描述出来需要完全新的概念. 一些奇异解次数为偶，所以他猜想（且大概能证明），以这种方式，所有充分大的偶次也能出现.

在同样的意义上，Andrew Bremner 能找到方程 $a^6+b^6+c^6=d^6+e^6+f^6$ 的"全部"参数解. 这里"全部"加引号，是因为这些解满足方程：

$$a^2+ad-d^2=f^2+fc-c^2,$$
$$b^2+be-e^2=d^2+da-a^2,$$
$$c^2+cf-f^2=e^2+eb-b^2$$

（这可能不象第一次出现时那么严格）. 他还能给出 $a^5+b^5+c^5=d^5+e^5+f^5$ 的"全部"参数解，满足 $a+b+c=d+e+f$ 和 $a-b=d-e$.

[1]B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves, II, *J. reine angew. Math.*, 218(1965), 79-108.

[2]Andrew-Bremner, Pythagorean triangles and a quartic surface, *J. reine angew. Math.*, 318(1980), 120-125.

[3]S. Brudno, Some new results on equal sums of like powers, *Math. Comput.*, 23(1969), 877-880.

[4]S. Brudno, On generating infinitely many solutions of the diophantine equation $A^6+B^6+C^6=D^6+E^6+F^6$, *Math. Comp.*, 24(1970), 453-454

[5]S. Brudno, Problem 4, *Proc. Number Theory Conf. Univ. of Colorado*, Boulder, 1972, 256-257.

[6] Simcha Brudno, Triples of sixth powers with equal sums, *Math. Comput.*, 30(1976), 646-648.

[7] S. Brudno and I. Kaplansky, Equal sums of sixth powers, *J. Number Theory*, 6(1974), 401-403.

[8] 曹珍富(Z. Cao), 丢番图方程引论, 第七章, 哈尔滨工业大学出版社, 1989; *MR* 92e:11018.

[9] Ajai Choudhry, The Diophantime equation $A^4+B^4=C^4+D^4$, *Indian J. Pure Appl. Math.*, 22(1991), 1:9-11; *MR* 92c:11024.

[10] V. A. Dem'janenko, L. Euler's conjecture (Russian), *Acta Arith.*, 25(1973/74), 127-135; *MR*50#12912.

[11] R. K. Guy, *Unsolved problems in number theory*, D1, Springer-Verlag, NewYork, 1981.

[12] Jan Kubiček, A simple new solution to the diophantine equation $A^3+B^3+C^3=D^3$ (Czech, German summary), *Časopis pěst. Mat.*, 99(1974), 177-178.

[13] L. J. Lander, Geometric aspects of diophantine equations involving equal sums of like powers, *Amer. Math. Monthly*, 75(1968), 1061-1073.

[14] L. J. Lander and T. R. Parkin, Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.*, 72(1966), 1079; *MR* 33# 554.

[15] L. J. Lander, T. R. Parkin, and J. L. Selfridge, A survey of equal sums of like powers, *math. Comput.*, 21(1967), 446-459; *MR* 36# 5060.

[16] R. Norrie, *Univ. of St. Andrews* 500*th Anniv. Mem.*, *Vol.*, Edinburgh, 1911, 89.

[17] Morgan Ward, Euler's three biquadrate problem, *Proc. Nat. Acad. Sci. U.S.A.*, 31(1945), 125-127; *MR*6, 259.

[18] Morgan Ward, Euler's problem on sums of three fourth powers, *Duke Math. J.*, 15(1948), 827-837; *MR*10, 283.

D2. Fermat 大定理及其相关的问题

Fermat 大定理是指：当 $n>2$ 时方程 $x^n+y^n=z^n$ 没有正整数解. 这是 1637 年左右 Fermat 写下的结论. 自此以后 360 年来，许

多数学家试图证明它，但均没有成功. 直到 1995 年 A. Wiles 发表了 100 多页的著名论文“模椭圆曲线与 Fermat 大定理”(Modular elliptic curves and Fermat's last Theorem)，才为证明 Fermat 大定理画上了句号. 两年后，Wiles 获得了为第一个证明 Fermat 大定理而设立的 Wolfskehl 奖. Wiles 的证明，是在前人工作的基础上进行的. 首先，Fermat 本人证明了 $n=4$ 时结论成立. 这样，证明 Fermat 大定理就只需要考虑 $n=p$ 为一个奇素数的情形. Euler 于 1770 年证明了 $p=3$ 的情形，后来 Gauss 对 $p=3$ 又给出了一个新证明. 基于上述结果，只需要证明：设 p 为一个奇素数，$p>3$，则不存在两两互素整数 a,b,c 满足 $a^p+b^p=c^p$，$abc\neq0$. 1985 年，Frey 建立了 Fermat 大定理与椭圆曲线的联系，构造了著名的 Frey 椭圆曲线 E：$y^2=x(x-a^p)(x+b^p)$. 1986 年，Ribet 证明：Fermat 大定理是椭圆曲线中的 Shimure-Taniyama 猜想的推论，即 Ribet 证明了 Frey 曲线 E 不满足 Shimure-Taniyama 猜想. 1995 年，A. Wiles 证明对“半稳定”(semi-stable)的椭圆曲线 Shimure-Taniyama 猜想成立. 由于可以不妨设 $a\equiv3\pmod4$，$2|b$，故 Fery 曲线 E 是半稳定的. 这样 Fermat 大定理作为 Wiles 上述结果的推论而得到证明.

对 Fermat 大定理的研究，还有一些重大的成果，例如历史上 Kummer，80 年代以来的 Faltings，Heath-Brown，特别是 Adleman 与 Heath-Brwon 合作对第一情形的重要工作.

现在，人们关心的问题是，除了给出 Fermat 大定理的新证明或简化证明外，对与其相关的一类问题将更为感兴趣. 这类问题包括：

(1)对每个正整数 c 判断方程 $x^4\pm y^4=cz^4$ 和 $x^4\pm y^4=cz^p$ 是否有 $(x,y)=1$ 的正整数解，这里 p 为奇素数. 显然当 $c=a^4+b^4$，$(a,b)=1$ 时方程 $x^4+y^4=cz^4$ 有解 $x=a,y=b,z=1$；利用 $x^4+y^4=a^4+b^4$ 含参数的解，可给出某些 c 使方程 $x^4+y^4=cz^4$ 有 $(x,y)=1,x>y$ 的两组正整数解. 例如当 $c=133^4+134^4$ 时，方程 $x^4+y^4=cz^4$ 有解 $z=1,(x,y)=(134,133),(158,59)$. 但对怎样的 c，方程可有三组正整数解？

Powell，Terai 和 Osada，曹珍富以及 Henri Darmon 还讨论了方程 $x^4 \pm y^4 = z^p$，$x^4 + dy^4 = z^p$ 以及 $cx^4 + dy^4 = z^p$，这里 $(x,y) = 1$，c 与 d 是两个互素的无平方因子正整数，p 是奇素数. 在 $p \nmid xyz$ 时最一般的结果是属于曹珍富的；在 $p \mid xyz$ 时，Darmon 在 Shimure-Taniyama 猜想的假设下，证明了：如果 $p \geq 11$，$p \equiv 1 \pmod 4$ 或 $2 \mid z$，则 $x^4 - y^4 = z^p(xyz \neq 0, (x,y) = 1)$ 没有整数解.

(2)对给定的正整数 A,B,C，研究方程 $Ax^n + By^n = Cz^n$ 满足 $(x,y)=1$ 的整数解. Darmon 和 Granvill 在有关椭圆曲线的 Serre 猜想和 Frey 猜想成立时，证明了当 $n>3$ 时方程 $Ax^n + By^n = Cz^n$ 仅有有限组整数解 (x,y,z,n). 但 Serre 猜想是很广的，例如 Serre 猜想能推出 Shimure-Taniyama 猜想. 他们还提出了“广义 Fermat 猜想”：方程

$$x^p + y^q = z^r, \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1, (x,y,z) = 1, xyz \neq 0$$

除 $1 + 2^3 = 3^2$，$2^5 + 7^2 = 3^4$，$7^3 + 13^2 = 2^9$，$2^7 + 17^3 = 71^2$，$3^5 + 11^4 = 122^2$，$17^7 + 76271^3 = 21063928^2$，$1414^3 + 2213459^2 = 65^7$，$9262^3 + 15312283^2 = 113^7$，$43^8 + 96222^3 = 30042907^2$，$33^8 + 1549034^2 = 15613^3$ 外，没有整数解.

Andrew Beal 对下列猜想的证明设了大奖：如果 p,q,r 均至少为 3，$(x,y,z)=1$，那么方程 $x^p + y^q = z^r$ 没有正整数解. 最近 Darmon 和 Merel 证明了：当 $p=q\geq 3$，$r=3$ 时 Beal 猜想成立.

Erdös 和 Oblath 证明了 $x^p \pm y^p = n!\,(p>2)$ 没有整数解. 我们希望证明方程 $x^n \pm y^n = n!\,Z^n (n>2)$ 没有 $z \neq 0$ 的整数解.

(3)初等方法在研究偶指数的 Fermat 问题中已获得了一系列结果. Terjanian 证明了：设 p 为奇素数，如果方程 $x^{2p} + y^{2p} = z^{2p}$ 有解，则 $2p \mid x$ 或 $2p \mid y$. 孙琦和曹珍富改进这个结果为 $8p \mid x$ 或 $8p \mid y$. 实际上，结合前人的工作，可以推出 $8p^3 \mid x$ 或 $8p^3 \mid y$. 曹珍富对于方程 $x^{2p} + y^{2p} = z^2$ 证明了 $4p^3 \mid x$ 或 $4p^3 \mid y$. 那么，是否可用初等方法给出 $x^{2p} + y^{2p} = z^{2p}$ 的最终解答？

[1]L. M. Adleman, and D. R. Heath-Brown, The first case of Fermat's last theorem, *Invent. Math.*, 79(1985), 409-416.

[2]Klaus Barner, Paul Wolfskehl and the Wolfskehl prize, Notices o the AMS, 44(1997), 10 1294−1303.

[3]曹珍富(Z. Cao), The Diophantine equation $cx^4 + dy^4 = z^p$, *C. R. Math. Rep. Acad. Sci. Canada*, 14(1992), 5: 231-234.

[4]曹珍富(Z. Cao), 关于 Fermat 大定理, 自然杂志, (I)10(1987), 5: 393−394, PЖ MaT., 1988, 1A178; (II)12(1989), 9: 718; (III)13(1990), 5: 314.

[5]曹珍富(Z. Cao), On the Diophantine equation $x^4 - py^2 = z^p$, *C. R. Math. Rep. Acad. Sci. Canada*, 17(1995), 2: 61 ~ 66; 18(1996), 5: 233 − 234.

[6]Henri Darmon, The equation $x^4 - y^4 = z^p$, *C. R. Math. Rep. Acad Sci. Canada*, 15(1993), 6: 286−291..

[7]H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.*, 27(1995), 513−543.

[8] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, preprint.

[9]Harold M. Edwards, *Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

[10]P. Erdős and R. Obláth, Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ and $n! \pm m! = x^p$, *Acta Litt. Sci. Szegcd*, 8(1937), 241-255; *Zbl.* 17. 004.

[11] G. Faltings, Endlich Keitssätze für abelsche Verietäten über Zahlkürpern, *Invent. Math.*, 73(1983), 349-366.

[12]G. Frey, Links between stable elliptic curves and certain diophantine equations, *Ann. Univ. Sarav.*, 1(1986), 1-40.

[13]D. R. Heath-Brown, Fermat's last theorem for "almost all" exponents, *Bull. London Math. Soc.*, 17(1985), 15-16.

[14]R. Daniel Mauldin, A generalization of Fermat's Last Theorem: the Beal conjecture and prize problem, *Notices of the AM S* 44(1997), 11: 1436−1437.

[15]B. Powell, Sur l'équation Diophantienne $x^4 \pm y^4 = z^p$, *Bull. Sc. Math.*, 107(1983), 219-223.

[16]Paulo Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, Heidelberg, Berlin, 1979; see *Bull. Amer. Math. Soc.*,

4(1981)218-222;*MR*81f:10023.

[17]K. A. Ribet, From the Taniyama-Shimura conjecture to Fermat's Last Theorem, *Ann. Fac. Sci. Toulouse Math.*, 11(1990), 116-139.

[18]K. A. Ribet, Wiles Proves Taniyama's Conjecture; Fermat's Last Theorem Follows, *Notices of AMS*, 40(1993), 6:575-576.

[19]孙琦(Q. Sun),曹珍富(Z. Cao),关于丢番图方程 $x^p - y^p = z^2$,数学年刊,A辑,7(1986),5:514—518; *MR* 88c:11022.

[20]N. Terai and H. Osada, The Diophantine equation $x^4 + dy^4 = z^p$, *C. R. Math. Rep. Acad. Sci. Canada*, 14(1992), 1:55-58.

[21]G. Terjanian, Sur l'équation $x^{2p} + y^{2p} = z^{2p}$, *C. R. Acad. Sci. Paris*, 285(1977), 973-975.

[22]Samuel S. Wagstaff, The irregular primes to 125000, *Math. Comp.*, 32(1978), 583-591; *MR* 58#10711.

[23]A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.*, 141(1995), 443—551.

D3. 垛形数问题

Mordell 问:方程

$$(A) \qquad 6y^2 = (x+1)(x^2 - x + 6)$$

是否仅有 $x = -1, 0, 2, 7, 15$ 和 74 的解?1971 年,Ljunggren 第一个给出了这一问题的回答,他证明方程 (A) 的全部解为 $x = -1$, 0,2,7,15,74 和 767. 后来,又有一些人给出了方程(A)的解的新证明. 但都不是初等的. 曹珍富希望给出(A)的一个初等证明.

注意到方程 (A) 来自 $y^2 = \binom{x}{0} + \binom{x}{1} + \binom{x}{2} + \binom{x}{3}$, Martin Gardner 取垛形数:三角形、四边形、四面体及方棱锥,并使其成对相等. 在因此而得到的六个问题中,除开"三角形=方棱锥"外,其余已全被解决了. 而此种情形导出的方程为:

$$3(2y+1)^2 = 8x^3 + 12x^2 + 4x + 3,$$

其解的数目是有限的. 那么它的解都由 $x = -1, 0, 1, 5, 6$ 和 85 给出吗?

"方棱锥=四边形"的情形是 Lucas 问题. 丢番图方程

$$y^2 = x(x+1)(2x+1)/6$$

仅有的非平凡解是 $x=24, y=70$ 吗？该问题已被 Watson 用椭圆函数和 Ljunggren(1952)用二次域上的 Pell 方程予以解决. 由于 Watson 和 Ljunggren 的方法不是初等的，Mordell 问：是否存在初等的证明. 马德刚，徐肇玉和曹珍富各自独立的给出了初等证明. 后来 Anglin 与 Cucurezeamu 各自给出了更为简短的初等证明.

对"四边形＝四面体"的情形，相应的方程为 $y^2=x(x+1)(x+2)/6$，是否(48,140)是仅有的非平凡解？因为前一个方程能写作为：

$$(2y)^2=2x(2x+1)(2x+2)/6,$$

故 $2|x$ 已得到解决. 而在 $2\nmid x$ 时，曹珍富已证明：方程 $2py^2=x(x+1)(x+2)$（p 为奇素数）仅有正整数解 $p=3, x=y=1$ 与 $p=7, x=7, y=6$，从而给出方程 $y^2=x(x+1)(x+2)/6$ 仅有非平凡解(48,140).

对"三角形数＝三角形的平方"，相应的方程为

$$(B)\qquad \frac{y(y-1)}{2}=\left(\frac{x(x-1)}{2}\right)^2.$$

Ljunggren(1946) 用 p-adic 方法证明了方程 (B) 仅有正整数解 $(x,y)=(1,1),(2,2),(4,9)$. 但 Ljunggren 的证明是一个"复杂的"证明. Cassels 利用四次域 $Q(\sqrt[4]{-2})$ 给出一个较为简单的证明. 曹珍富、邓谋杰与黎进香又给出一个更为简洁且初等的证明.

[1]W. S. Anglin, The Square Pyramid Puzzle, *Amer. Math. Monthly*, 97 (1990), 120-124.

[2]J. W. S. Cassels, Integral points on certain elliptic curves, *Proc. London Math. Soc.*, 14A(1965), 3: 55-57.

[3]曹珍富(Z. Cao)，邓谋杰，黎进香，关于方程 $\left(\frac{x(x-1)}{2}\right)^2=\frac{y(y-1)}{2}$ 的初等解法，科学通报，39(1994)，7: 670.

[4]I. Cucurezeanu, An Elementary Solution of Lucas' Problem, *J. Number Theory*, 44(1993), 9-12.

[5]H. E. Dudeney, *Amusements in Mathematics*, Nelson, 1917, 26, 167.

[6]Raphael Finkelstein, On a diophantine equation with no non-trivial integral solution, *Amer. Math. Monthly*, 73 (1966), 471-477.
[7]W. Ljunggren, Solution compléte de quelques équations du sixiéme degré á deux indéterminées, *Arch. Math. Naturv.*, 48(1946), 7:26-29.
[8]W. Ljunggren, New solution of a problem proposed by E. Lucas, *Norsk Mat. Tidskr.*, 34(1952), 65-72.
[9]W. Ljunggren, A diophantine Problem, *J. London Math. Soc.*, 3(1971), 385-391.
[10]E. Lucas, Problem 1180, *Nouv. Ann. Math.*, 14(1875), 2:336.
[11]马德刚(D. Ma), 方程 $6y^2 = x(x+1)(2x+1)$ 的解的初等证明, 四川大学学报(自然科学版), 1985, 4:107－116.
[12]C. N. Watson, The problem of the square pyramid, *Messenger of Math.*, 48(1918/19), 1-22.
[13]徐肇玉(Z. Xu), 曹珍富(Z. Cao), 关于 Mordell 的一个问题, 科学通报, 30(1985), 7:558－559.

D4. l 个 k 次幂的和表整数

假设 $r_{k,l}(n)$ 是 $n = \sum_{i=1}^{l} x_i^k$ 取正整数 x_i 的解的个数, Hardy 和 Littlewood 的猜想 K 为: $\varepsilon > 0$ 推出 $r_{k,k}(n) = O(n^{\varepsilon})$. 对 $k = 2$, 这是众所周知的. 事实上, 对充分大的 n,

$$r_{2,2}(n) < n^{(1+\varepsilon)\ln 2/\ln\ln n}$$

且这里的 ln2 不能被更小的数代替(否则上式不成立). Mahler 对 $k = 3$ 否定了这一猜想, 他证明了 $r_{3,3}(n) > c_1 n^{1/12}$ 对无穷多个 n 成立. Erdős 认为, 对所有 n, $r_{3,3}(n) < c_2 n^{1/12}$ 是可能的, 但没有人能证明. 猜想 K 也许对 $k \geqslant 3$ 不成立, 而 $\sum_{n=1}^{x} (r_{k,k}(n))^2 < x^{1+\varepsilon}$ 对充分大 x 是可能成立的.

S. Chowla 证明了, 对 $k \geqslant 5$, $r_{k,k}(n) \neq O(1)$, 并和 Erdős 一起证明了, 对每个 $k \geqslant 2$ 和无穷多个 n, 有

$$r_{k,k}(n) > \exp(c_k \ln n / \ln\ln n).$$

Mordell 证明了 $r_{3,2}(n) \neq O(1)$ 且 Mahler 证明了 $r_{3,2}(n) > (\ln n)^{1/4}$ 对无穷多个 n 成立. $r_{3,2}(n)$ 的非平凡的上界现尚不清楚. Jean Lagrange 已证明, $\limsup r_{4,2}(n) \geqslant 2$ 且 $\limsup r_{4,3}(n) = \infty$.

设 $A_{k,l}(x)$ 是整数 $n \leqslant x$ 能被表成 l 个 k 次幂的和的个数. 一个棘手的问题是估计 $A_{k,l}(x)$ 的大小. Landau 证明了,

$$A_{2,2}(x) = (c + o(1))x/(\ln x)^{1/2}.$$

Erdös 和 Mahler 证明了,如果 $k > 2$,那么 $A_{k,2} > c_k x^{2/k}$,且 Hooley 证明了 $A_{k,2} = (c_k + o(1))x^{2/k}$. 似乎可以肯定,如果 $l < k$,那么 $A_{k,l} > c_{k,l}x^{l/k}$,且 $A_{k,k} > x^{1-\epsilon}$ 对每一个 ϵ 成立,但是这些尚未被证实.

从 Chowla-Erdös 的结果知,对所有 k,存在 n_k 使得

$$n_k = p^3 + q^3 + r^3$$

解的个数比 k 大. 对多于 3 个加数的情形,现在还没有得到任何相应的结果.

另一个引人注目的问题是:每一个数都是 4 个立方数的和吗?已证明除开形如 $9n \pm 4$ 的数外,这是正确的.

更进一步的要求是,每一个数是 4 个立方数的和,而其中的两个立方数相等. 特别地, $76 = x^3 + y^3 + 2z^3$ 有解吗?其他小于 1000 且仍存疑问的数是 148, 183, 230, 253, 356, 418, 428, 445, 482, 491, 519, 580, 671, 734, 788, 923, 931 和 967. 所有不具有 $9n \pm 4$ 形式的数都是 3 个立方数的和吗?

方程 $3 = x^3 + y^3 + z^3$ 有解 $(1,1,1)$, $(4,4,5)$, $(4,-5,4)$ 和 $(-5,4,4)$,还有其他解吗? Cassels 证明,如果存在解,则 $x \equiv y \equiv z \pmod 9$. 对于方程 $x^3 + y^3 + z^3 + w^3 = 0$,从曹珍富的书《丢番图方程引论》(248 - 252 页)中得知,早在 1830 年 Baba 就给出了参数解 $x = (s^6 - 4)s$, $y = -(s^6 + 8)s$, $z = s^6 + 6s^3 - 4$, $w = -s^6 + 6s^3 + 4$. 后来, Kroneck, Osborn 等又给出了含三个、两个参数的解. 1988 年,范绍舲给出了一般的解 $x = am - bn$, $y = -(bm + an + bn)$, $z = -(dm - cn)$, $w = -(cm + dm + dn)$,其中 a, b, c, d 是任意整数,

$$m = (a + 2b)(a^2 + ab + b^2) - (c - d)(c^2 + cd + d^2),$$

$$n = \begin{cases} (a - b)(a^2 + ab + b^2) - \\ (c + 2d)(c^2 + cd + d^2), & 当 m \neq 0, \\ 1 & 当 m = 0. \end{cases}$$

[1]J. W. S. Cassels, A note on the Diophantine Equation $x^3 + y^3 + z^3 = 3$, *Math. Comp.*, 44(1985), 265-266.

[2]曹珍富(Z. Cao), 丢番图方程引论, 哈尔滨工业大学出版社, 1989, 248-252; *MR* 92e: 11018.

[3]S. Chowla, The number of representations of a large number as a sum of nonnegative *n*th powers, *Indian Phys.-Math. J.*, 6(1935), 65 - 68; *Zbl.* 12. 339.

[4]H. Davenport, Sums of three positive cubes, *J. London Math. Soc.*, 25(1950), 339-343; *MR* 12, 393.

[5]范绍舲(S. Fan), 不定方程 $w^3 + x^3 + y^3 + z^3 = 0$, 自然杂志, 11(1988), 9: 710.

[6]W. J. Ellison, Waring's problem, *Amer. Math. Monthly*, 78 (1971), 10-36.

[7]P. Erdős, On the representation of an integer as the sum of k kth powers, *J. London Math. Soc.*, 11(1936), 133-136; *Zbl.* 13. 390.

[8]P. Erdős, On the sum and difference of squares of primes Ⅰ, Ⅱ, *J. London Math. Soc.*, 12(1937), 133-136, 168-171; *Zbl.* 16. 201, 17. 103.

[9]P. Erdős and K. Mahler, On the number of integers which can be represented by a binary form, *J. London Math. Soc.*, 13(1938), 134-139.

[10]P. Erdős and E. Szemeredi, On the number of solutions of $m = \sum_{i=1}^{k} x_i^k$, *Proc. Symp. Pure Math.*, 24 Amer. Math. Soc., Providence, 1972, 83-90.

[11]V. L. Gardiner, R. B. Lazarus, and P. R. Stein, Solutions of the diophantine equation $x^3 + y^3 = z^3 - d$, *Math. Comp.*, 18(1964), 408-413; *MR*31 # 119.

[12]G. H. Hardy and J. E. Littlewood, Partitio Numerorum VI: Further re-

searches in Waring's problem, *Math. Z.*, 23(1925), 1-37.

[13]柯召(Chao Ko), Decompositions into four cubes, *J. London Math. Soc.*, 11(1936), 218-219.

[14]Jean Lagrange, Thése d'Etat de l'Université de Reims, 1976.

[15]M. Lal, W. Russell, and W. J. Blundon, A note on sums of four cubes, *Math. Comp.*, 23(1969), 423-424; *MR* 39#6819.

[16]K. Mahler, Note on hypothesis K of Hardy and Littlewood, *J. London. Math. Soc.*, 11(1936), 136-138.

[17]K. Mahler, On the lattice points on curves of genus 1, *Proc. London Math. Soc.*, 39(1935), 431-466.

[18]A. Makowski, Sur quelques problémes concernant les sommes de quatre cubes, *Acta Arith.*, 5(1959), 121-123; *MR* 21# 5609.

[19]J. C. P. Miller, M. F. C. Woollett, Solutions of the diophantine equation $x^3+y^3+z^3=k$, *J. London Math. Soc.*, 30(1955), 101-110; *MR* 16, 979.

[20]A. Schinzel and W. Sierpinski, Sur les sommes de quatre cubes, *Acta Arith.*, 4 (1958), 20-30.

D5. 二元四次丢番图方程问题

Ljunggren 已证明,方程 $x^2=2y^4-1$ 仅有的正整数解为(1,1)和(239,13),但是他的证明是复杂且深刻的. Mordell 问:是否能找到一个简单的或初等的证明?

Ljunggren 和其他的人对同类方程作了相当可观的研究. 一些参考文献选编在下面. 其中 Cohn 对全部 $D\leqslant 400$ 的情形,给出了方程 $y^2=Dx^4+1$ 的全部解. 曹珍富对方程 $x^4-Dy^2=-1$ 证明了:设 $\eta=u_0+v_0\sqrt{D}$ 是 Pell 方程 $u^2-Dv^2=-1$ 的基本解,且设 $u_0=du_1^2$, d 无平方因子,则有 $x^2+y\sqrt{D}=\eta^d$. 乐茂华用 Baker 方法证明了:如果 $D>\exp 64$,那么方程 $x^4-Dy^2=1$ 最多只有一个正整数解. 在此之前,对任意 D, Ljunggren 证明了 $x^4-Dy^2=1$ 最多有两组正整数解,且当 $D=1785$ 时,方程恰有两组正

整数解 $x=13, y=4$ 和 $x=239, y=1352$. 对于方程 $x^4-Dy^2=k$ 与 $x^2-Dy^4=k(|k|\neq 1,4)$，目前仅解决一些特例，例如 Cohn (1968) 证明 $x^4-5y^2=-44$ 仅有正整数解 $(x,y)=(1,3),(3,5),(47,1453)$；$x^4-5y^2=11$ 仅有整数解 $(2,1),(4,7)$；$x^2-5y^4=44$ 仅有正整数解 $(7,1)$；$x^2-5y^4=11$ 仅有正整数解 $(4,1),(56,5)$；$x^2-5y^4=-44$ 仅有正整数解 $(6,2),(19,3),(181,9)$. Tzanakis 证明了 $x^2-3y^4=46$ 仅有正整数解 $(7,1),(17,3)$，因而最终解决了当 $|n|\leqslant 100$ 时方程 $x^4-4x^2y^2+y^4=n$ 的求解问题. 曹珍富在 $|n|\leqslant 200$ 时也解决了这个问题，此时主要解决了两个 n 值：-194 与 193. 但是方程 $x^2-3y^4=-194$ 与方程 $x^2-3y^4=193$ 的解如何？能否给出它们的全部解？已知的部分解为：$x^2-3y^4=-194$ 有部分解 $(7,3),(41,5),(1586297,957)$；$x^2-3y^4=193$ 有部分解 $(14,1),(31,4),(86,7),(79321,214)$.

[1]Edward A. Bender and Norman P. Herzberg, Some diophantine equations related to the quadratic form ax^2+by^2, *Bull. Amer. Math. Soc.*, 81(1975), 161-162.

[2]J. Blass, On the diophantine equation $Y^2+K=X^5$, *Bull. Amer. Math. Soc.*, 80(1974), 329.

[3]曹珍富(Z. Cao)，关于丢番图方程 $x^4-Dy^2=1$，哈尔滨工业大学学报，(Ⅰ)1981, 4:53-58;(Ⅱ)1983, 2:133-138;(Ⅲ)(与贾广聚)哈尔滨师范大学学报(自然科学版)，1985, 1:78—82.

[4]曹珍富(Z. Cao)，关于丢番图方程 $x^2+1=2y^2, x^2-1=2Dz^2$，数学杂志，3(1983), 3:227—235; *MR* 85*j*:11032.

[5]曹珍富(Z. Cao)，一些 Diophantus 方程的研究，自然杂志，10(1987), 2:151；哈尔滨工业大学学报，1988, 3:1—7; *MR* 90*k*:11026.

[6]J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.*, 39(1964), 537-540; *MR* 29# 1166.

[7]J. H. E. Cohn, The diophantine equation $y^2=Dx^4+1$, Ⅰ, *J. London Math. Soc.*, 42(1967), 475-476; *MR* 35 # 4158; Ⅱ, *Acta Arith.*, 28(1975/76), 273-275; *MR* 52 # 8029; Ⅲ, *Math. Scand.*, 42(1978), 180-

188.

[8]J. H. E. Cohn, Some quartic Diophantine equation, *Pacific. J. Math.*, 26(1968), 2:233-243.

[9]J. H. E. Cohn, The diophantine equation $x^4 - Dy^2 = 1$, *Quart. J. Math. Oxford*, 26 (1975), 3:279-281.

[10]J. H. E. Cohn, Five diophantine equations, *Math. Scand.*, 21(1967), 61-70.

[11]J. H. E. Cohn, Eight diophantine equations, *Proc. London Math. Soc.*, 16(1966), 153-166; Addendum, *ibid*, 17(1967), 381.

[12]N. P. Herzberg, Integer solutions of $by^2 + p^n = x^3$, *J. Number Theory*, 7(1975), 221-234; *Zbl.* 302.10021.

[13]柯召(C. Ko), 孙琦(Q. Sun), 关于不定方程 $x^4 - Dy^2 = 1$, 四川大学学报(自然科学版), 1975, 1:57 — 61.

[14]柯召(C. Ko), 孙琦(Q. Sun), 关于丢番图方程 $x^4 - Dy^2 = 1$, (Ⅰ) 四川大学学报(自然科学版), 1979, 1:1 — 4; 数学学报, 23(1980), 6:922 — 926; (Ⅱ)数学年刊, A 辑, 1(1980), 1:83-88.

[15]柯召(C. Ko), 孙琦(Q. Sun), 关于丢番图方程 $x^4 - 2py^2 = 1$, 四川大学学报(自然科学版), 1979, 4:5—9; 1983, 2:1—3.

[16]柯召(C. Ko), 孙琦(Q. Sun), 关于丢番图方程 $x^4 - pqy^2 = 1$, (Ⅰ)科学通报, 24(1979), 16:721—723; (Ⅱ)四川大学学报(自然科学版), 1980, 3:37—43.

[17]柯召(C. Ko), 孙琦(Q. Sun), 关于丢番图方程 $x^2 - Dy^4 = 1$, 数学年刊, A 辑, 2(1981), 4:491 — 495.

[18]乐茂华(M. Le), A note on the diophantine equation $x^{2p} - Dy^2 = 1$, *Proc. Amer. Math. Soc.*, 107(1989), 1: 27-34.

[19]D. J. Lewis, Two classes of diophantine equations, *Pacific J. Math.*, 11(1961), 1063-1076.

[20]W. Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo*, Ⅰ, 5(1942)#5, 27pp; *MR* 8, 6.

[21]W. Ljunggren, Über die Gleichung $x^4 - Dy^2 = 1$, *Arch. Math. Naturv.*, 45(1942), 5:61—70.

[22]W. Ljunggren, On a diophantine equation, *Norske Vid. Selsk. Forh.*

Trondheim, 18(1945), 125-128; *MR* 8, 136.

[23]W. Ljunggren, New theorems concerning the diophantine equation $Cx^2 + D = y^n$, *Norske Vid. Selsk. Forh. Trondheim*, 29(1956), 1-4; *MR*17, 1185

[24]W. Ljunggren, On the diophantine equation $Cx^2 + D = y^n$, *Pacific J. Math.*, 14(1964), 585-596; *MR* 28#5035.

[25]W. Ljunggren, Some remarks on the diophantine equation $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$, *J. London Math. Soc.*, 41(1966), 542-544; *MR* 33#5555.

[26]L. J. Mordell, The diophantine equation $y^2 = Dy^4 + 1$, *J. London Math. Soc.*, 39(1964), 161-164; *MR* 29#65.

[27]T. Nagell, Contributions to the theory of a category of diophantine equations of the second degree with two unknowns, *Novd Acta Soc. Sci. Upsal.*, (4)16(1955)#2; 38pp; *MR* 17, 13.

[28]N. Tzanakis, The Diophantine equation $x^2 - Dy^4 = k$, *Acta Arith.*, 46 (1986), 257-269.

[29]朱卫三(W. Zhu), $x^4 - Dy^2 = 1$ 可解的充要条件, 数学学报, 28(1985), 5: 681—683.

D6. 连续数问题

Leo Moser 证明方程

$$1^n + 2^n + \cdots + (m-1)^n = m^n$$

在 $m < 10^{10^6}$ 时没有非平凡解(平凡解显然有1+2=3). 后来 Rufus Bowen 猜想该方程没有非平凡解. 易知,若该方程成立,则 $n \sim m \ln 2$. 事实上,阎发湘证明了该方程成立可推出 $m = \left[\frac{n-1}{\ln 2}\right] + 3$.

利用原根很容易证明该方程可推出 $m-1$ 无平方因子,设 $m-1 = p_1 \cdots p_s$, $p_i (i = 1, \cdots, s)$ 是不同的素数,则有 $(p_i - 1) | n (i = 1, \cdots, s)$ 且 $p_1 \cdots p_{i-1} p_{i+1} \cdots p_s + 1 \equiv 0 \pmod{p_i} (i = 1, \cdots, s)$. 由曹珍富等关于方程 $\sum_{j=1}^{s} \frac{1}{x_j} + \frac{1}{x_1 \cdots x_s} = 1$ 的解可知,方程 $1^n + 2^n + \cdots + (m-1)^n = m^n$ 推出 $m-1$ 至少是8个不同素数的乘积. Robert

Tijdeman 注意到关于方程

$$1^n + 2^n + \cdots + k^n = m^n$$

的一般结果不蕴含上述特定的方程，并且给出下面的最近进展．

van de Lune 证明了，如果$(m-1)^n < \frac{1}{2}m^n$，则

$$(L) \qquad 1^n + 2^n + \cdots + (m-1)^n < m^n.$$

Best 和 te Riele 证明了，如果 $(m-2)^n \geqslant \frac{1}{2}(m-1)^n$，则

$$(M) \qquad 1^n + 2^n + \cdots + (m-1)^n > m^n.$$

因此，我们可以假设，对于任意大的 m，整数 n 可由

$$\left(1-\frac{1}{m}\right)^n > \frac{1}{2} > \left(1-\frac{1}{m-1}\right)^n$$

来确定．Erdös 猜想，(L) 和(M) 两者均无限多次成立．van de Lune 和 te Riele 证明了，(M) 对几乎所有的 m 成立．Best 和 te Riele 证明了，(L) 对 $m \leqslant x$ 的最多 $\ln x$ 个值成立．他们计算了33对使 (L) 成立的(m,n)，最小的一对是：

$$m = 1121626023352385, n = 777451915729368.$$

但要证明 (L) 无限多次成立似乎很困难．

柯召和孙琦研究了比 Bowen 猜想更一般的 Escott 方程

$$x^n + (x+1)^n + \cdots + (x+h)^n = (x+h+1)^n,$$

证明了该方程在 $1 \leqslant n \leqslant 33$ 时仅有正整数解 $1+2=3, 3^2+4^2=5^2$ 以及 $3^3+4^3+5^3=6^3$，而在 $n>33$ 时，柯召，孙琦和邹兆南完全解决了 n 为奇数的情形，即他们证明了此时方程无其他的解．他们猜想 $n>33$ 为偶数时也无正整数解．

[1]M. R. Best and H. J. J. te Riele, On a conjecture of Erdös concerning sums of powers of integers, *Report NW* 23/76, Mathematisch Centrum Amsterdam, 1976.

[2]曹珍富(Z. Cao)，刘锐(R. Liu)，张良瑞(L. Zhang)，关于不定方程 $\sum_{j=1}^{s}\frac{1}{x_j} + \frac{1}{x_1\cdots x_s} = 1$ 和 Znám 问题，自然杂志，12(1989)，7：554－555.

[3]曹珍富(Z. Cao),刘锐(R. Liu),张良瑞(L. Zhang),On the equation $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=1$ and Znám's problem, *J. Number Theory*,27(1987),2:206-211. *MR* 89d:11023.

[4]P. Erdős, Advanced probAlem 4347, *Amer. Math. Monthly*,56(1949),343.

[5]K. Győry, R. Tijdeman and M. Voorhoeve, On the equation $1^k+2^k+\cdots+x^k=y^z$, *Acta Arith.*,37(1980),233-240.

[6]柯召(C. Ko),孙琦(Q. Sun),关于方程 $x^n+(x+1)^n+\cdots+(x+h)^n=(x+h+1)^n$,四川大学学报(自然科学版),1962,2:9—18.

[7]柯召(C. Ko),孙琦(Q. Sun)和邹兆南,关于方程 $\sum_{j=0}^{h}(x+j)^n=(x+h+1)^n$,四川大学学报(自然科学版),1978,2—3:19—24.

[8]J. van de Lune, On a conjecture of Erdős (I), *Report ZW* 54/75, Mathematisch Centrum, Amsterdam, 1975.

[9]J. van de Lunc and H. J. J. te Riele, On a conjecture of Erdős (I), *Report ZW* 56/75, Mathematisch Centrum, Amsterdam, 1975.

[10]L. Moser, On the diophantine equation $1^n+2^n+\cdots+(m-1)^n=m^n$, *Scripta Math.*,19(1953),84-88; *MR* 14,950.

[11]J. J. Schäffer, The equation $1^p+2^p+\cdots+n^p=m^q$, *Acta Math.*,95(1956),155-189; *MR* 17,1187.

[12]M. Voorhoeve, K. Győry and R. Tijdeman, On the diophantine equation $1^k+2^k+\cdots+x^k+R(x)=y^z$, *Acta Math.*,143(1979),1-8; *MR* 80e:10020.

[13]阎发湘(F. Yan),关于 Bowen 猜想,辽宁大学学报(自然科学版),1980,1:1—10.

D7. 方程 $x^3+y^3+z^3=x+y+z$

Wunderlich 问,方程 $x^3+y^3+z^3=x+y+z$ 的解(参量表示)怎样?Bernstein, S. Chowla, Edgar, Fraenkel, Oppenheim, Segal 和 Sierpinski 已给出了一些解,其中一些是参量形式的,因此

一定存在无穷多个解.然而,通解仍未得到.

[1]Leon Bernstein, Explicit solutions of pyramidal Diophantine equations, *Canad. Math. Bull.*, 15(1972), 177-184; *MR* 46#3442.

[2]Hugh Maxwell Edgar, Some remarks on the Diophantine equation $x^3+y^3+z^3=x+y+z$, *Proc. Amer. Math. Soc.*, 16(1965), 148-153; *MR* 30#1094.

[3]A. S. Fraenkel, Diophantine equations involving generalized triangular and tetrahedral numbers, in *Computers in Number Theory, Proc. Allas Symp. No.* 2, Oxford 1969 Academic Press, London and New York (1971), 99-114.

[4]A. Oppenheim, On the Diophantine equation $x^3+y^3+z^3=x+y+z$, *Proc. Amer. Math. Soc.*, 17(1966), 493-496; *MR* 32#5590.

[5]A. Oppenheim, On the diophantine equation $x^3+y^3-z^3=px+py-pz$, *Univ. Beograd Publ. Elektrotehn. Fak. Ser.* #235(1968); *MR* 39#126.

[6]S. L. Segal, A note on pyramidal numbers, *Amer. Math. Monthly*. 69(1962), 637-638; *Zbl.* 105, 36.

[7]W. Sierpinski, Sur une propriété des nombres tétraédraux, *Elem. Math.*. 17(1962), 29-30; *MR* 24#A3118.

[8]W. Sierpinski, Trois nombres tétraédraux en progression arithmetique, *Elem. Math.*, 18(1963), 54-55; *MR* 26#4957.

[9]M. Wunderlich, Certain properties of pyramidal and figurate numbers, *Math. Comp.*, 16(1962), 482-486; *MR* 26#6115.

D8. 两个幂之差

1842年,Catalan 曾猜想:2^3和3^2是仅有的两个连续数都是正整数的幂(幂>1).两个正整数幂中有一个是平方数的情形吸引了很多数学家的注意,最后在1962年由柯召证明了此时 Catalan 猜想成立.后来,Chein, Rotkiewicz 和曹珍富分别给出柯召定理的一个简化证明.1976年,Tijdeman 用 Baker 方法基本上解决了 Catalan 猜想,即如果有两个连续数都是正整数的幂,那么每个正整数的幂均小于

一个绝对常数 c. 近来 c 还可被具体定出，例如 $c < 10^{10^{500}}$. Cassels，柯召还分别独立地证明了不存在三个连续数都是正整数的幂. 这个结论可由下面的结论推出：方程 $x^p + 1 = y^q$（q 是素数，p 是奇素数）有正整数解，推出 $p|y$ 且 $q|x$.

更一般地，如果 $a_1 = 4, a_2 = 8, a_3 = 9, \cdots$ 是具有这样幂的序列，那么，Choodnowski 宣布已证明 $a_{n+1} - a_n$ 随 n 趋于无穷. Erdös 猜想 $a_{n+1} - a_n > c' n^c$，但目前还没有证明它的希望.

Jan Mycielski 注意到，除开与2同余(mod 4)的那些数外，所有的数均能表成每个均大于4的两个幂之差. 他问6，14或34是否也能这样表达. 对于更一般的情形 $a^x - b^y = (2p^s)^z$，这里 p 为奇素数，s 为非负整数，曹珍富证明了在 $(a,b) \equiv (5,3),(3,5),(\pm 3, 7),(7, \pm 3) \pmod 8$ 时除 $3^4 - 7^2 = 2^5, (4p^{4s}+1)^2 - (4p^{4s}-1)^2 = (2p^s)^4$ 外无 $z \geqslant 4$ 的非负整数解. Perisastri，曹珍富，Toyoizumi 以及曹珍富与王笃正等还讨论了 $s = 1$ 的若干情形.

Erdös 问是否有无穷多个数不具有 $x^k - y^l$ 的形式，其中 $k > 1, l > 1$.

Carl Rudnick 用 $N(r)$ 代表 $x^4 - y^4 = r$ 的正整数解的个数，并且问 $N(r)$ 是否有界. H. Hansraj Gupta 注意到，Herdy 和 Wright 给出了 $x^4 - y^4 = u^4 - v^4$ 的参数解，这些解表明，$N(r)$ 是 0，1 或无穷多次地取 2. 例如 $133^4 - 59^4 = 158^4 - 134^4 = 300783360$. 如果 $N(r) = 3$，那么 r 必定是非常非常地大. 但是几乎没有任何疑问，$N(r)$ 是有界的.

Hugh Edgar 问，给定素数 p, q 和整数 h，$p^m - q^n = 2^h$ 有多少解 (m,n)？是否至多 1 个？仅有有限个吗？例如，$3^2 - 2^3 = 2^0, 5^3 - 11^2 = 2^2, 5^2 - 3^2 = 2^4$. 曹珍富在给出方程 $x^2 + 2^m = y^n (n > 1)$ 的全部解的基础上，和王笃正一起证明了：对于素数 p, q 和整数 h，方程 $p^m - q^n = 2^h$ 最多有一组 $m > 1, n > 0$ 的解. 他对给定素数 p，q，还证明方程 $p^m - q^n = 2^h$ 最多有一组 $m > 1, n > 0, h > 0$ 的解. 如果存在整数 a, b, h' 满足 $p = qa^2 + 2^{h'} b^2, h' \equiv h \pmod 2$，$b \neq$

0，那么方程 $p^m - q^n = 2^h$(p,q 是素数)无 $m > 1$ 的正整数解. 他猜想：存在正常数 A，当 $\max(a,b,c) > A$ 时，方程 $a^x + b^y = c^z$(a,b,c 是不同的素数)最多有一组正整数解 x,y,z. 当 $\max(a,b,c) > 13$ 与 $z > 1$ 时已证明猜想是对的. 对于 $13 < \max(a,b,c) < 200$. 他给出了 $a^x + b^y = c^z$ 的全部 解，由此证明此时猜想也是对的.

[1]曹珍富(Z. Cao)，方程 $a^x - b^y = (2p^t)^z$ 和 Hugh Edgar 问题，科学通报，30(1985)，14：1116—1117；哈尔滨工业大学学报，1986，3：7—11；*MR* 88a：11029.

[2]曹珍富(Z. Cao)，关于方程 $a^x - b^y = 10^z$，扬州师院学报(自然科学版)，1986，1：17—20.

[3]曹珍富(Z. Cao)，王笃正(D. Wang)，关于丢番图方程 $a^x - b^y = (2p)^z$，扬州师院学报(自然科学版)，1987，4：25—30；*MR* 90c：11020.

[4]曹珍富(Z. Cao)，方程 $x^2 + 2^m = y^n$ 和 Hugh Edgar 问题，科学通报，31(1986)，7：555—556.

[5]曹珍富(Z. Cao)，王笃正(D. Wang)，关于 Hugh Edgar 问题，科学通报，32(1987)，14：1043—1046.

[6]曹珍富(Z. Cao)，关于 Diophantus 方程 $a^x + b^y = c^z$(Ⅰ)，科学通报，31(1986)，22：1688-1690；(Ⅱ)科学通报，33(1988)，3：237.

[7]曹珍富(Z. Cao)，On the Diophantine equation $ax^2 + by^2 = p^z$，*J. Harbin Inst. Tech.*，23(1991)，6：108-111；*MR* 94a：11041.

[8]曹珍富(Z. Cao)，数论中的若干新的结果和问题，河池师专学报，1987，1：1—8.

[9]曹珍富(Z. Cao)，形为 $a^x + b^y = c^z$ 的指数丢番图方程，哈尔滨工业大学学报，1987，4：113 — 121；*MR* 89k：11016.

[10]曹珍富(Z. Cao)，佟瑞洲(R. Tong)，王镇江(Z. Wang)，关于指数 Diophantus 方程的一个猜想，自然杂志，14(1991)，11：872—873.

[11]曹珍富(Z. Cao)，柯召定理的一个证明，西南师大学报(自然科学版)，1987，2：16—19.

[12]J. W. S. Cassels，On the equation $a^x - b^y = 1$，Ⅱ，*Proc. Comb. Phil. Soc.*，56 (1960)，97-103.

[13]E. Z. Chein, A note on $x^2 = y^q + 1$, *Proc. Amer. Math. Soc.*, 56(1976), 83-84.

[14]柯召(C. Ko),关于方程 $x^2 = y^n + 1, xy \neq 0$,四川大学学报(自然科学版),1962,1:1－6; On the diophantine equation $x^2 = y^n + 1, xy \neq 0$, *Sci. Sin.* (Notes),14(1964),457-460.

[15]柯召(C. Ko),关于连续数的一个问题,四川大学学报(自然科学版),1962,2:1－6.

[16]M. Perisastri, A note on the equation $a^x - b^y = 10^z$, *Math. Stud.*, 37(1969),211-212.

[17]A. Rotkiewicz, Applications of Jacobi's symbol to Lehmer's numbers, *Acta Arith.*, 42(1983),163-187.

[18]R. Tijdeman, On the equation of Catalan, *Acta Arith.*, 29(1976), 197-209; *MR*53#7941.

[19]M. Toyoizumi, On the equation $a^x - b^y = (2p)^z$, *Math. Stud.*, 46(2-4)(1978),113-115(1982); *MR* 84h:10025.

D9. 一些指数丢番图方程

Brenner 和 Foster 提出下列一般问题:设$\{p_i\}$是素数的有限集合,$\varepsilon_i = \pm 1$. 什么时候,指数丢番图方程 $\sum \varepsilon_i p_i^{x_i} = 0$ 能用初等方法(即模算术)来解?更确切地,对于给定的 p_i, ε_i,确定是否存在一个模 M 使得给定的方程与同余式$\sum \varepsilon_i p_i^{x_i} \equiv 0 \pmod M$等价?他们已解决了许多特殊的情形,其中大部分情形是素数 p_i 为4个且小于108. 在少数几种情形里,纵使素数 p_i 中有两个相等,初等方法也有效,但是,一般来说,初等方法无效. 事实上,$3^a = 1 + 2^b + 2^c$ 和 $2^a + 3^b = 2^c + 3^d$ 都不能用简单同余法来解. 但用 Pell 方程方法曹珍富给出了这两个方程非常简短的解答. 对于有限单群的 p- 主块寻常不可约特征标的次数方程 $1 + p^a = 2^b q^c + 2^d p^e q^f$,这里 p, q 是奇素数,a, b, c, d, e, f 是非负整数, L. J. Alex 和 Foster 证明了$(p,q) = (73,223)$ 或$(223,73)$时,仅有平凡解$(t,0,0,0,t,0)$;曹珍富证明了在$(p,q) \equiv (1,7) \pmod{12}$且 $\left(\frac{q}{p}\right) = 1$ 时仅有

平凡解$(t,0,0,0,t,0)$. 他还一般地证明了 $x^2 = p^n - p^m + 1(p > 5$ 是素数) 仅有 $m = n$ 的正整数解. 在曹珍富的书《丢番图方程引论》(368 — 370 页) 中还介绍了 Alex 给出的方程 $1 + 2^a = 3^b 5^c + 2^d 3^e 5^f, 1 + 3^a = 2^b 5^c + 2^d 3^e 5^f, 1 + 5^a = 2^b 3^c + 2^d 3^e 5^f$ 的全部非负整数解.

Hugh Edgar 问,除开 $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$ 外,方程 $1 + q + q^2 + \cdots + q^{x-1} = p^y$ 还有其它的解吗?这里 p,q 为奇素数且 $x \geqslant 5, y \geqslant 2$. 我们知道, Ljunggren 曾证明方程 $\frac{x^n - 1}{x - 1} = y^2 (n \geqslant 4)$ 仅有正整数解 $\frac{7^4 - 1}{7 - 1} = 20^2$ 和 $\frac{3^5 - 1}{3 - 1} = 11^2$(这一结果的初等证明已由曹珍富给出). 因此, Hugh Edgar 问题当 $2|y$ 时仅有解 $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$. 对于 $2\nmid y$, 曹珍富证明它有解的充要条件是 1) 方程 $x^2 + p(q-1)y^2 = q^z$ 有正整数解, 且 2) 设 z_1 是满足 $x_1^2 + p(q-1)y_1^2 = q^{z_1} (x_1 > 0, y_1 > 0)$ 的最小正整数, 则 $x_1 = 1, y_1 = p^{(y-1)/2}, z_1 = x$. 由此推出, 对给定的素数 p,q 方程 $1 + q + q^2 + q^3 + \cdots + q^{x-1} = p^y$ 最多只有一组解 $x \geqslant 5, y \geqslant 2$. 另一个由 Pell 方程基本解表示的充要条件也被给出来了.

对指数丢番图方程 $a^x + b^y = c^z$, 当 a,b,c 是不同的素数时, 从 1958 年 Nagell 开始, 经过 Makowski, Hadano, Uchiyama, 孙琦与周小明, 杨晓卓的共同努力(见曹珍富的书《丢番图方程引论》, 361—362页), 到1985年给出了 $\max(a,b,c) \leqslant 23$ 时的全部解. 曹珍富给出了 $23 < \max(a,b,c) < 200$ 的全部解以及一些理论结果(参见 D8). 当 a,b,c 是商高数组时, Jesmanowicz 有一个著名的猜想, 并且有过许多工作(见 D28).

对 Ramanujan—Nagell 方程 $x^2 + 7 = 2^n$ 以及各种推广, 许多数学家均饶有兴味. 1960年, Apéry 证明了方程

$$x^2 + D = 2^n, 2 \nmid D > 0 \qquad (A)$$

在 $D \neq 7$ 时最多有两组正整数解 x,n. Browkin 和 Schinzel 提出如下猜想: 方程 (A) 有两组正整数解当且仅当 $D = 23$, 或 $D = 2^k$

$-1, k>3$. 1967 年，Schinzel 部分地解决了这个猜想，证明了除 $D=2^k-1$ 外，方程(A)在 $n>80$ 时最多有一组正整数解. 1981 年，Beukers 完全解决了 Browkin-Schinzel 猜想，即证明了该猜想成立. 同时 Beukers 还讨论了方程

$$(B) \qquad x^2-D=2^n, 2\nmid D>0$$

的解. 显然

Ⅰ. 当 $D=2^{2k}-3\cdot 2^{k+1}+1, k\geqslant 3$ 时，方程(B)有解$(x,n)=(2^k-3,3),(2^k-1,k+2),(2^k+1,k+3),(3\cdot 2^k-1,2k+3)$；

Ⅱ. 当 $D=2^{2l}+2^{2k}-2^{k+l}-2^{k+1}-2^{l+1}+1, k>1, l\geqslant k+1$ 时，方程(B)有解$(x,n)=(2^l-2^k-1,k+2),(2^l-2^k+1,l+2),(2^k+2^l-1,k+l+2)$；

Ⅲ. 当 $D=\left(\dfrac{2^{l-2}-17}{3}\right)^2-32, 2\nmid l\geqslant 9$ 时，方程(B)有解$(x,n)=\left(\dfrac{2^{l-2}-17}{3},5\right),\left(\dfrac{2^{l-2}+1}{3},l\right)$和$\left(\dfrac{17\cdot 2^{l-2}-1}{3},2l+1\right)$.

Beukers 证明：方程(B)最多有四组正整数解，且除Ⅰ，Ⅱ和Ⅲ的情形外，方程(B)最多有三组正整数解. 由此知Ⅰ的情形给出的解是(B)的全部正整数解. 乐茂华证明：Ⅱ，Ⅲ情形给出的解也是(B)的全部正整数解，且除Ⅰ，Ⅱ，Ⅲ外，如果 Pell 方程 $X^2-DY^2=-1$ 有整数解，则(B)最多只有两组正整数解. Beukers 在 $D<10^{12}$ 时，证明了：除Ⅰ，Ⅱ，Ⅲ外方程(B)最多只有两组正整数解，并给出 $|D|<1000$ 时方程(A)与(B)有两个或多于两个正整数解的全体 D 的索引(参阅曹珍富的书 375—376 页).

对于 $p>2$ 是一个素数，Apéry 证明了当 $D>0$ 时方程

$$(C) \qquad x^2+D=p^n, p\nmid D$$

最多只有两组正整数解. Beukers 证明：当 $-D$ 不是平方数，$D<0$ 时，如果方程(C)有两组正整数解$(x,n)=(A,k),(A',k'),k'>k$，则 $p^k\leqslant\max(2\cdot 10^6,600D^2)$；同时他还证明方程$(C)$在 $D<0$ 时最多只有四组正整数解. 乐茂华在 $D<0$ 且 $\max(-D,p)\geqslant 10^{190}$ 时证明了方程(C)最多有三组正整数解. Toyoizumi，孙琦与曹珍

富，乐茂华等人还讨论了方程 $x^2 + D^m = p^n (D > 0)$ 的解，参看D28. 曹珍富利用二次域的理论研究了更为广泛的丢番图方程 $Cx^2 + 2^{2m}D = k^n$，例如证明了 $3x^2 + 8 = 11^n$ 仅有正整数解 $(x, n) = (1, 1), (21, 3)$；$5x^2 + 16 = 21^n$ 仅有正整数解 $(x, n) = (1, 1), (43, 3)$；$13x^2 + 40 = 53^n$ 仅有正整数解 $(x, n) = (1, 1), (107, 3)$，等等. 容易看出，结合 Baker 方法还可以得出另外一些新结果.

[1]Leo J. Alex, Problem E 2880, *Amer. Math. Monthly*, 89(1981), 291.

[2]L. J. Alex and L. L. Foster, On the Diophantine equations of the form $1 + 2^a = p^b q^c + 2^d p^e q^f$, *Rocky Mountain J. Math.*, 13(1983), 2:321-331.

[3]R. Apéry, Sur une équation diophantienne, *C. R. Acad. Sci. Paris, Sér. A*, 251(1960), 1263-1264; 1451-1452.

[4] F. Beukers, On the generalized Ramanujan-Nagell equation, I, *Acta Arith.*, 38(1980/81), 389-410; II, *Acta Arith.*, 39(1981), 113-123.

[5]J. L. Brenner and Lorraine L. Foster, Exponential diophantine equations, *Pacific J. Math.*, 101(1982), 2:263-301.

[6]J. Browkin and A. Schinzel, On the equation $2^n - D = y^2$, *Bull. Acad. Polon. Sci.*, Sér. Sci. Math. Astronom. Phys., 8(1960), 311-318.

[7]曹珍富(Z. Cao)，丢番图方程引论，哈尔滨工业大学出版社，1989；*MR* 92e:11018.

[8]曹珍富(Z. Cao), On the Diophantine equation $\frac{ax^m - 1}{abx - 1} = by^2$, *Chinese Sci. Bull.* 36(1991), 4:275-278; *MR* 92k:11035.

[9]曹珍富(Z. Cao)，吴波(B. Wu)，关于丢番图方程 $\frac{x^n - 1}{x - 1} = y^2$ 的一个初等解法与 Edgar 方程，《青年科技论文集》，黑龙江科技出版社，1990，3—7.

[10]曹珍富(Z. Cao)，有限单群中的一类丢番图方程，东北数学(待发表).

[11]曹珍富(Z. Cao)，关于丢番图方程 $Cx^2 + 2^{2m}D = k^n$，数学年刊，A 辑，15(1994)，2:235—240.

[12]乐茂华(M. Le), On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = 2^{n+2}$, *Acta Arith.*, 60(1991), 2:149-167; *MR* 92m:11030.

[13]乐茂华(M. Le),关于丢番图方程 $x^2-D=p^n$ 的解数,数学学报,34(1991),3:378—387.

[14]W. Ljunggren, Some theorems on indeterminate equations $\frac{x^n-1}{x-1}=y^q$, *Norsk Mal. Tidsskr.*, 25(1943), 17-20.

[15]A. Schinzel, On two theorems of Gelfond and some of their applications, *Acta Arith.*, 13(1967), 177-236.

D10. **埃及分数问题**

埃及分数即单位分数,指分子为1的分数. Rhind Papyrus 是流传到今最古老的数学之一,它涉及到有理数表成单位分数和的问题:

$$\frac{m}{n}=\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}.$$

在这方面已提出了大量的问题,其中许多尚未解决,并且还继续不断地提出新的问题. 因此,对埃及分数的兴趣持久不衰. 我们已给出了许多参考文献,但这也只是它的一部分. Bleicher 对这一专题给出了一个详细的综述,且把注意力集中在各种算法上. 这些算法被提出来用以构造给定类型的表示,如 Fibonacci—Sylvester 算法,Erdös 算法,Golomb 算法,Bleicher 自己的两个算法,Farey 级数算法及连分数算法等. 在曹珍富的书《丢番图方程引论》的第十章中,选择了该专题的几个问题作了专门介绍.

Erdös 和 Straus 猜想:方程

$$\frac{4}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$$

对于所有 $n>1$ 有正整数解. 后来 Straus 发现,当 $n>2$ 时如果猜想成立,那么 $x\neq y, y\neq z, z\neq x$. 在 Mordell 的书中,已证明除开 n 为素数且与$1^2, 11^2, 13^2, 17^2, 19^2$或$23^2$同余(mod 840)的情形外,该猜想为真. Bernstein, Obláth, Rosati, Shapiro, Yamamoto 以及 Nicola Franceschine 都对此作了研究,证明了猜想对 $n\leqslant 10^8$ 成立. Schinzel 已注意到人们可表示

$$\frac{4}{at+b}=\frac{1}{x(t)}+\frac{1}{y(t)}+\frac{1}{z(t)},$$

其中 $x(t),y(t),z(t)$ 是关于 t 的整数多项式，且假定 b 不是 a 的二次剩余．以上可参看 Mordell 的书 Diophantine equations.

Sierpinski 对方程

$$\frac{5}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z},$$

作了一个相应的猜想. Palama 证实它对 $n\leqslant 922321$ 成立. Stewart 改进到 $n\leqslant 1057438801$ 和所有不具有 $278460k+1$ 形式的 n.

Schinzel 放宽 x,y,z 必须为正的条件，用一般的 m 代替 4 和 5，且要它仅对 $n>n_m$ 成立. n_m 可能比 m 大的例子是 $n_{18}=23$. 该猜想已相继为 Schinzel，Sierpinski，Sedláček，Palama 和 Stewart，及 Webb 证明对越来越大的 m 成立. 他们还证明了 $m<36$ 时，该猜想成立. Breusch 和 Stewart 独立地证明了，如果 $\frac{m}{n}>0$ 且 n 为奇，那么 $\frac{m}{n}$ 是有限个奇整数的倒数和. 请参见 Graham 的论文. Vaughan 已证明，如果 $E_m(N)$ 表不大于 N 且使 $\frac{m}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$ 没有解的 n 的个数，那么，

$$E_m(N)\ll N\cdot\exp\{-c(\ln N)^{2/3}\},$$

其中 c 仅取决于 m. 后来单墫把这一结果推广到 $s(\geqslant 3)$ 个变元上.

与 Breusch 和 Stewart 的结果相比，由 Stein，Selfridge，Graham 和其他人提出的下列问题仍未获解决：如果有理数 $\frac{m}{n}$（n 为奇）能被表成 $\sum\frac{1}{x_i}$，其中 x_i 相继被选作可能的最小正的奇整数，且满足取定每个奇整数后留下的部分是非负的，那么和的项数总是有限的吗？例如：

$$\frac{2}{7}=\frac{1}{5}+\frac{1}{13}+\frac{1}{115}+\frac{1}{10465}.$$

John Leech 在77年3月14日给 R. K. Guy 的一封信中问，关于倒数和为1的不同奇整数集合，人们知道些什么呢？如：

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{15}+\frac{1}{21}+\frac{1}{27}+\frac{1}{35}+\frac{1}{63}+\frac{1}{105}+\frac{1}{135}=1,$$

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}+\frac{1}{33}+\frac{1}{35}+\frac{1}{45}+\frac{1}{55}+\frac{1}{77}+\frac{1}{105}=1$$

他说，至少需要集合中的9个数，而且最大的分母至少应为105. 注意此问题与 Sierpinski 伪完全数(B2)

$$945=315+189+135+105+63+45+35+27+15+9+7$$

的联系. 已知 m/n(n 为奇)总可表为不同奇单位分数的和. Erdős 置 $\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}=\frac{a}{b}$，其中 $b=[2,3,\cdots,n]$ 是 $2,3,\cdots,n$ 的最小公倍数. 他发现 $\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$，且 $\frac{1}{2}+\frac{1}{3}+\frac{1}{4}=\frac{13}{12}$ 使得 $a\pm 1\equiv 0 \pmod b$，因此，他问是否还有这样的情形？他猜想没有. 此外 $(a,b)=1$ 能出现无穷多次吗？

如果 $\sum_{i=1}^{t}\frac{1}{x_i}=1$ 且 $x_1<x_2<x_3<\cdots$ 为不同的正整数，Erdős 和 Graham 问 $m(t)=\min\max x_i$ 为多少？其中 min 取遍所有集合 $\{x_i\}$. 例如，$m(3)=6$，$m(4)=12$，$m(12)=120$. $m(t)<ct$ 对某些常数 c 成立吗？

借用上一段的符号，那么对所有 i，$x_{i+1}-x_i\leqslant 2$ 可能成立吗？Erdős 猜想它为不可能，并为此问题的解决提出10美元的奖金.

给定一有正密率的序列 $x_1,x_2,\cdots$，总存在有限个子集 $\{x_{i_k}\}$ 使得 $\sum\frac{1}{x_{i_k}}=1$ 吗？如果 $x_i<ci$ 对所有 i 成立，那么存在这样的子集

吗?Erdős 再次为此问题的解决提供10美元的奖励. 如果 $\lim\inf \frac{x_i}{i} < \infty$, 他强烈地猜想, 答案是否定的, 并为此问题的解决提供5美元的奖励.

定义 $N(t)$ 为使 $\sum_{i=1}^{t} \frac{1}{x_i} = 1$ 的解 $(x_1,\cdots,x_t)$ 的个数, 定义 $M(t)$ 为不同的解满足 $x_1 \leqslant \cdots \leqslant x_t$ 的个数, Singmaster 计算出:

t	1	2	3	4	5	6
$M(t)$	1	1	3	14	147	3462
$N(t)$	1	1	10	215	12231	2025462

Erdős 问 $M(t)$ 和 $N(t)$ 的渐近式是什么?柯召, 孙琦和曹珍富等曾大力地讨论了 x_t 是其它 $t-1$ 个 x_i 乘积的情形, 即 $\sum_{i=1}^{s} \frac{1}{x_i} + \frac{1}{x_1\cdots x_s} = 1$. 其中不失一般可设 $1 < x_1 < \cdots < x_s$, 解的个数用 $\Omega(s)$ 表示. 柯召和孙琦给出 $\Omega(s) = 1(1 \leqslant s \leqslant 4)$, $\Omega(5) = 3$, $\Omega(6) = 8$. Janák 和 Skula 也得到当 $s \leqslant 6$ 时的全部解及 $\Omega(7) \geqslant 18$. 曹珍富, 刘锐和张良瑞用计算机证明了 $\Omega(7) = 26$.①这个方程是否有素数解(指 $x_1,\cdots,x_s$ 均为素数的解)显然与 Bowen 猜想(见 D6)、Giuga 问题(见 A17)以及素数同余式组(A18)等有联系. 1964年, 柯召, 孙琦猜想该方程至少有一个素数解; 1987年, 曹珍富, 刘锐与张良瑞猜想: 该方程至多有一个素数解. 当 $1 \leqslant s \leqslant 7$ 时, 已知的结果是: 该方程恰有一个素数解. 对于 $\Omega(s)$ 的估计也有一系列工作, 例如孙琦和曹珍富证明了 $\Omega(s+1) \geqslant \Omega(s) + \sum_{j=1}^{\Omega(s-1)} (\frac{d(k_j)}{2} - 1)$, 这里 $k_j = (x_1^{(j)}\cdots x_{s-1}^{(j)})^2 + 1$, $(x_1^{(j)},\cdots,x_{s-1}^{(j)})$ 为 $\sum_{i=1}^{s-1} \frac{1}{x_i} + \frac{1}{x_1\cdots x_{s-1}} = 1$ 的 $\Omega(s-1)$ 个解. 从这个关系, 他们先后构造性证明了: 当 $s \geqslant 4$ 时, $\Omega(s+1) > \Omega(s)$; 当 $s \geqslant 10$ 时 $\Omega(s+1) \geqslant \Omega(s) + 3$; 当 $s \geqslant 10$ 时

① 参考文献[15]中漏了三组解. [17]中给出了全部解.

$\Omega(s+1) \geqslant \Omega(s)+5$；当 $s \geqslant 10$ 时 $\Omega(s+1) \geqslant \Omega(s)+8$. 1988 年，曹珍富证明了：当 $s \geqslant 11$ 时，$\Omega(s+1) \geqslant \Omega(s)+17$，且当 $s \geqslant 11$，$2 \nmid s$ 时，$\Omega(s+1) \geqslant \Omega(s)+23$，并且构造了 $\Omega(9) \geqslant 62$，$\Omega(10) \geqslant 74$. 最近，曹珍富等又证明了当 $s \geqslant 11$ 时，$\Omega(s+1) \geqslant \Omega(s)+39$ 且当 $2 \nmid s \geqslant 11$ 时 $\Omega(s+1) \geqslant \Omega(s)+57$. 但是，$\Omega(s)$ 的渐近公式仍未得到. 另外，曹珍富问：方程 $\sum_{i=1}^{s} \frac{1}{x_i}+\frac{1}{x_1 \cdots x_s}=2(1<x_1<\cdots<x_s)$ 是否有解？是否对任意给定正整数 $x_1>1$，都存在正常数 c，当 $n \geqslant c$ 时，方程 $\sum_{i=1}^{s} \frac{1}{x_i}+\frac{1}{x_1 \cdots x_s}=1(1<x_1<\cdots<x_s)$ 都有整数解？对 $\Omega(s)$，曹珍富猜想：存在正常数 c，在 $\min(s, t)>c$ 时有 $\Omega(s+t+1) \geqslant \Omega(s+t)+\Omega(s)+s$.

关于 $\Omega(s)$ 与 Znám 问题(F31)的关系参见 F31. 另一个类似的问题见 D26.

Graham 已证明，如果 $n>77$，则可把 n 分成 t 个不同正整数的和，即 $n=x_1+x_2+\cdots+x_t$ 使得 $\sum_{i=1}^{t} \frac{1}{x_i}=1$. 更一般地，对于任意的正有理数 α, β，必存在正整数 $r(\alpha, \beta)$，我们取其为最小数，它使得任意比 r 大的整数都能分成比 β 大的不同整数的和，而其倒数和取 α. 关于 $r(\alpha, \beta)$，除开 D. H. Lehmer 未发表的工作证明了，77 不能以这种方式分解，因而 $r(1,1)=77$ 外，其他的结果很少.

Graham 猜想，对充分大 n(10^4 左右?)，我们类似地能分 $n=x_1^2+x_2^2+\cdots+x_t^2$ 使 $\sum_{i=1}^{t} \frac{1}{x_i}=1$. 我们也能分解 $n=p(x_1)+p(x_2)+\cdots+p(x_t)$，其中 $p(x)$ 是“合理”多项式，例如 x^2+x 不是合理的，因为它仅取偶数.

L.-S. Hahn 问，如果正整数以任意方式分成有限个集合，那么这些集合中总存在 s 个集合，任意的正有理数均能表成 s 个集合中的一个集合的有限个不同元素的倒数和吗？特别地，$s=1$ 时，此问题是否正确？如果 $s=1$ 时不正确，那么 s 为多少时问题的回答是

肯定的？

Erdös 设

$$1=\frac{1}{x_1}+\cdots+\frac{1}{x_k}, \text{其中 } x_1<x_2<\cdots<x_k,$$

并且问，如果 k 固定，那么 $\max x_1=?$ 如果 k 变化，那么 x_k 的最大值是多少？冯克勤，魏权龄和刘木兰证明了 $\max x_k=M_1\cdots M_{k-1}$，这里 $M_1=2, M_{i+1}=M_1\cdots M_i+1(i\geqslant 1)$.

Nagell 证明了，算术级数的倒数和决不是整数，参看 Erdös 和 Niven 的论文以及曹珍富编著的讲义《数论及其应用》(哈尔滨工业大学教材，1985).

[1] A. V. Aho and N. J. A. Sloane, Some doubly exponential sequences, *Fibonacci Quart.*, 11(1973), 429-438; *MR*49#209.

[2] A. Aigner, Brüche als Summe von Stammbrüchen, *J. reine angew. Math.*, 214/215(1964), 174-179.

[3] P. J. van Albada and J. H. van Lint, Reciprocal bases for the integers, *Amer. Math. Monthly*, 70(1963), 170-174.

[4] E. J. Barbeau, Computer Challenge corner: Problem 477: A brute force program, *J. Recreational Math.*, 9(1976/77), 30.

[5] E. J. Barbeau, Expressing one as a sum of distinct reciprocals: comments and a bibliography, *Eureka* (Ottawa), 3(1977), 178-181.

[6] Leon Bernstein, Zur Lösung der diophantischen Gleichung $m/n=1/x+1/y+1/z$ insbesondere im Falle $m=4$, *J. reine angew. Math.*, 211(1962), 1-10; *MR* 26#77

[7] M. N. Bleicher, A new algorithm for the expansion of Egyptian fractions, *J. Number Theory*, 4(1972), 342-382; *MR* 48#2052.

[8] M. N. Bleicher and P. Erdös, The number of distinct subsums of $\sum_1^N 1/i$, *Math. Comp.*, 29(1975), 29-42(and see *Notices Amer. Math. Soc.*, 20(1973) A-516)

[9] M. N. Bleicher and P. Erdös, Denominators of Egyptian fractions, *J. Number Theory*, 8(1976), 157-168; *MR* 53#7925; II, *Illinois J. Math.*,

20(1976),598-613;*MR* 54#7359.

[10]Robert Breusch, A special case of Egyptian fractions, Solution to Advanced Problem 4512, *Amer. Math. Monthly*, 61(1954), 200-201.

[11]W. S. Burnside, *Theory of Groups of Finite Order*, 2nd ed. Cambridge University Press, London, 1911, reprinted Dover, New York, 1955, Note A, 461-462.

[12]N. Burshtein, On distinct unit fractions whose sum equals 1, *Diserete Math.*, 5(1973), 201-206.

[13]Paul J. Campbell, Bibliography of algorithms for Egyptian fractions (preprint) Beloit Coll. Beloit W I 53511, U. S. A.

[14]J. W. S. Cassels, On the representation of integers as the sum of distinct summands taken from a fixed set , *Acta Sci. Math. Szeged*, 21(1960), 111-124

[15]曹珍富(Z. Cao),刘锐(R. Liu),张良瑞(L. Zhang),On the equation $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=1$ and Znám's Problem, *J. Number Theory*, 27(1987), 2: 206-211; *MR* 89d: 11023.

[16]曹珍富(Z. Cao),On the number of solutions of the Diophantine equation $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=1$,纪念华罗庚数论与分析国际学术会议,1988年,北京.

[17]曹珍富(Z. Cao),刘锐,张良瑞,关于不定方程 $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=1$ 和 Znám 问题,自然杂志,12(1989),7:554—555.

[18]曹珍富(Z. Cao),荆成明,关于 Znám 问题解数,哈尔滨工业大学学报(待发表).

[19]A. B. Chace, *The Rhind Mathematical Papyrus*, M. A. A., Oberlin, 1927.

[20]Robert Cohen, Egyptian fraction expansions, *Math. Mag.*, 46(1973), 76-80; *MR* 47#3300.

[21]D. Culpin and D. Griffiths, Egyptian fractions, *Math. Gaz.*, 63(1979), 49-51; *MR* 80d: 10014.

[22] D. R. Curtiss, On Kellogg' s Diophantine problem, *Amer. Math. Monthly*, 29(1922), 380-387.

[23] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Diophantine Analysis, Chelsea, New York, 1952, 688-691.

[24] P. Erdös, Egy Kürschák-féle elemi számelméleti tétel áltadanositasa, *Mat. es Phys. Lapok*, 39(1932).

[25] P. Erdös, On arithmetical properties of Lambert series, *J. Indian Math. Soc.*, 12(1948), 63-66.

[26] P. Erdös, On a diophantine equation (Hungarian. Russian and English summaries), *Mat. Lapok*, 1(1950), 192-210; *MR* 13, 208.

[27] P. Erdös, On the irrationality of certain series, *Nederl. Akad. Wetensch. (Indag. Math.)*, 60(1957), 212-219.

[28] P. Erdös, Sur certaines séries á valeur irrationnelle, *Enseignement Math.*, 4(1958), 93-100.

[29] P. Erdös, *Quelques Problémes de la Théorie des Nombres*, Monographie de 1'Enseignement Math. No. 6, Geneva, 1963, problems 72-74.

[30] P. Erdös, Comment on problem E2427, *Amer. Math. Monthly*, 81 (1974), 780-782.

[31] Paul Erdös, Some problems and results on the irrationality of the sum of infinite series, *J. Math. Sci.*, 10(1975), 1-7.

[32] Paul Erdös and Ivan Niven, Some properties of partial sums of the harmonic series, *Bull. Amer. Math. Soc.*, 52(1946), 248-251; *MR* 7, 413.

[33] P. Erdös and S. Stein, Sums of distinct unit fractions, *Proc. Amer. Math. Soc.*, 14(1963), 126-131.

[34] P. Erdös and E. G. Straus, On the irrationality of certain Ahmes series, *J. Indian Math. Soc.*, 27(1968), 129-133.

[35] P. Erdös and E. G. Straus, Some number theoretic results, *Pacific J. Math.*, 36(1971), 635-646.

[36] P. Erdös and E. G. Straus, Solution of problem E2232, *Amer. Math. Monthly*, 78(1971), 302-303.

[37] P. Erdös and E. G. Straus, On the irrationality of certain series, *Pacific J. Math.* 55(1974), 85-92; *MR* 51 # 3069.

[38]P. Erdős and E. G. Straus, Solution to problem 387, *Nieuw Arch. Wisk.*, 23(1975), 183.

[39]冯克勤(K. Feng), 魏权龄和刘木兰, 关于 Kulkarni 问题和 Erdős 一个猜想, 科学通报, 32(1987), 3: 164—168.

[40]Nicola Franceschine , Egyptian Fractions, MA Dissertation, Sonoma State Coll. CA, 1978.

[41]S. W. Golomb, An algebraic algorithm for the representation problems of the Ahmes papyrus, *Amer. Math. Monthly*, 69(1962), 785-786.

[42]S. W. Golomb, On the sums of the reciprocals of the Fermat numbers and related irrationalities, *Canad. J. Math.*, 15(1963), 475-478.

[43] R. L. Graham, A theorem on partitions, *J. Austral. Math. Soc.*, 4(1963), 435-441.

[44]R. L. Graham, On finite sums of unit fractions, *Proc. London Math. Soc.*, (3)14(1964), 193-207; *MR* 28#3968.

[45]R. L. Graham, On finite sums of reciprocals of distinct nth powers, *Pacific J. Math.*, 14(1964), 85-92; *MR* 28#3004.

[46]L.-S. Hahn, Problem E2689, *Amer. Math. Monthly*, 85(1978), 47.

[47]J. W. Hille, Decomposing fractions, *Math. Gaz.*, 62(1978), 51-52.

[48] Ludwig Holzer, *Zahlentheorie Teil* Ⅱ, Ausgewählte Kapitel der Zahlentheorie, Math.-Nat. Bibl. No. 14a, B. G. Teubner-Verlag, Leipzig, 1965, Sect. A, 1-27; *MR* 34#4186.

[49]J. Janák, and L. Skula, On the integers x_i for which $x_i | x_1 \cdots x_{i-1} x_{i+1} \cdots x_n + 1$ holds, *Math. Slovaca*, 28(1978), 305-310.

[50]Dag Magne Johannessen, On unit fractions Ⅱ, *Nordisk mat. Tidskr.*, 25-26(1978), 85-90; *MR* 80a: 10010; *Zbl.* 384. 10004.

[51]Dag Magne Johannessen and T. V. Söhus, On unit fractions Ⅰ, *ibid*, 22(1974), 103-107; *MR* 55#252; *Zbl.* 291. 10010.

[52]Ralph W. Jollensten, A note on the Egyptian problem, *Congressus Numerantium XVII*, Proc. 7th S. E. Conf. Combin. Graph Theory, Comput., 1976, 351-364, *MR* 55#2746.

[53] O. D. Kellogg, On a diophantine problem, *Amer. Math. Monthly*, 28(1921), 300-303.

[54]E. Kiss, Quelques remarques sur une équation diophantienne (Romanian. French summary), *Acad. R. P. Romine Fil. Cluj, Stud. Cerc. Mat.*, 10(1959), 59-62.

[55]E. Kiss, Remarques relatives à la représentation des fractions subunitaires en somme des fractions ayant le numerateur égal á 1'unité (Romanian), *Acad. R. P. Romine Fil. Cluj, Stud. Cerc. Mat.*, 11(1960), 319-323.

[56]柯召(C. Ko), 孙琦(Q. Sun), 关于单位分数表1问题, 四川大学学报(自然科学版), 1964, 1:13—29.

[57]Ladis D. Kovach, Ancient algorithms adapted to modern computers, *Math. Mag.*, 37(1964), 159-165.

[58]József Kürschák, A harmonikus sorról, *Mat. es. Phys. Lapok*, 27(1918), 299-300.

[59] Denis Lawson, Ancient Egypt revisited, *Math. Gaz.*, 54(1970), 293-296; *MR* 58# 10697.

[60]P. Montgomery, Solution to Problem E2689, *Amer. Math. Monthly*, 86(1979), 224.

[61]L. J. Mordell, *Diophantine Equtions*, Academic Press, London, 1969, 287-290.

[62]T. Nagell, *Skr. Norske Vid. Akad. Kristiania* I, 1923, no. 13(1924), 10-15.

[63]M. Nakayama, On the decomposition of a rational number into "Stammbrüche," *Tôhoku Math. J.*, 46(1939), 1-21.

[64]James R. Newman, The Rhind Papyrus, in *The World of Mathematics*, Allen and Unwin, London, 1960, 169-178.

[65]R. Obláth, Sur 1'équation diophantienne $4/n = 1/x_1 + 1/x_2 + 1/x_3$, *Mathesis*, 59(1950), 308-316; *MR* 12, 481.

[66]J. C. Owings, Another proof of the Egyptian fraction theorem, *Amer. Math. Monthly*, 75(1968), 777-778.

[67]G. Palamà, Su di una congettura di Sierpinski relativa alla possibilità in numeri naturali della $5/n = 1/x_1 + 1/x_2 + 1/x_3$, *Boll. Un. Mat. Ital.*, (3)13(1958), 65-72; *MR* 20# 3821.

[68]G. Palamá, Su di una congettura di Schinzel, *Boll. Un. Mat. Ital.*,

(3)14 (1959),82-94;*MR* 22# 7989.

[69]T. E. Peet, *The Rhind Mathematical Papyrus*, Univ. Press of Liverpool, London, 1923.

[70]L. Pisano, *Scritti*, Vol. 1, B. Boncompagni, Rome, 1857.

[71]Y. Rav, On the representation of a rational number as a sum of a fixed number of unit fractions, *J. reine angew. Math.*, 222(1966), 207-213.

[72]L. A. Rosati, Sull'equazione diofantea $4/n = 1/x_1 + 1/x_2 + 1/x_3$, *Boll. Un. Mat. Ital.*, (3)9(1954), 59-63; *MR* 15, 684.

[73]H. D. Ruderman, Problem E2232, *Amer. Math. Monthly*, 77(1970), 403.

[74]Harry Ruderman, Bounds for Egyptian fraction partitions of unity, Problem E2427, *Amer. Math. Monthly*, 80(1973), 807.

[75]H. E. Salzer, The approximation of numbers as sums of reciprocals, *Amer. Math. Monthly*, 54(1947), 135-142; *MR* 8, 534.

[76]H. E. Salzer, Further remarks on the approximation of numbers as sums of reciprocals, *Amer. Math. Monthly*, 55(1948), 350-356; *MR* 10, 18.

[77]单墫(Z. Shan), On the Diophantine equation $\sum_{i=0}^{k} \frac{1}{x_i} = \frac{a}{n}$, 数学年刊, B辑, 7(1986), 2:213—220.

[78]Andrzerj Schinzel, Sur quelques propriétés des nombres $3/n$ te $4/n$, où n est un nombre impair, *Mathesis*, 65(1956), 219-222; *MR* 18, 284.

[79]Jiri Sedláček, Über die Stammbrüche, *Časopis Pěst. Mat.*, 84(1959), 188-197; *MR* 23# A829.

[80]Ernest S. Selmer, Unit fraction expansions and a multiplicative analog, *Nordisk mat. Tidskr.*, 25-26(1978), 91-109; *Zbl.* 384. 10005.

[81]W. Sierpinski, Sur les décompositions de nombres rationnels en fractions primaires, *Mathesis*, 65(1956), 16-32; *MR* 17, 1185.

[82]W. Sierpinski, *On the Decomposition of Rational Numbers into Unit Fractions* (Polish), Pánstwowe Wydawnictwo Naukowe, Warsaw, 1957.

[83]W. Sierpinski, Sur une algorithme pour le développer les nombres réels en séries rapidement convergentes, *Bull. Int. Acad. Sci. Cracovie Ser. A Sci. Mat.*, 8(1911), 113-117.

[84]David Singmaster, The number of representations of one as a sum of u-

nit fractions(mimeographed note)1972.

[85]N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973.

[86]B. M. Stewart, Sums of distinct divisors, *Amer. J. Math.*, 76(1954), 779-785; *MR*16, 336.

[87]B. M. Stewart, *Theory of Numbers*, Macmillan, N. Y., 1964, 198-207.

[88]B. M. Stewart and W. A. Webb, Sums of fractions with bounded numerators, *Canad. J. Math.*, 18(1966), 999-1003; *MR* 33#7297.

[89]E. G. Straus and M. V. Subbarao, On the representation of fractions as sum and difference of three simple fractions, *Congressus Numeratium XX*, Proc. 7th Conf. Numerical Math. Comput. Manitoba 1977, 561-579.

[90]孙琦(Q. Sun),关于单位分数表1的表法个数,四川大学学报(自然科学版),1978,2—3:15—18.

[91]孙琦(Q. Sun),曹珍富(Z. Cao),关于方程 $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=1$,数学研究与评论,7(1987),1:125 — 128; *MR* 89b:11029.

[92]孙琦(Q. Sun),曹珍富(Z. Cao),On the Equation $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=n$ and the Number of Solutins of Znám's Problem,数学进展,15(1986),3:329—330; *MR* 89j:1105.

[93]J. J. Sylvester, On a point in the theory of vulgar fractions, *Amer. J. Math.*, 3(1880), 332-335, 388-389.

[94]D. G. Terzi, On a conjecture of Erdős-Straus, *BIT*, 11(1971), 212-216.

[95]L. Theisinger, Bemerkung über die harmonische Reihe, *Monat. für Math. u. Physik*, 26(1915), 132-134.

[96]R. C. Vaughan, On a problem of Erdős, Straus and Schinzel, *Mathematika*, 17(1970), 193-198.

[97]C. Viola, On the diophantine equations $\prod_0^k x_i-\sum_0^k x_i=n$ and $\sum_0^k 1/x_i=a/n$, *Acta Arith.*, 22(1972/73), 339-352.

[98]W. A. Webb, On $4/n=1/x+1/y+1/z$, *Proc. Amer. Math. Soc.*, 25(1970), 578-584.

[99]William A. Webb, Rationals not expressible as a sum of three unit frac-

tions, *Elem. Math.*, 29(1974), 1-6.

[100]William A. Webb, On a theorem of Rav concerning Egyptian fractions, *Canad. Math. Bull.*, 18(1975), 155-156.

[101]William A. Webb, On the unsolvability of $k/n = 1/x + 1/y + 1/z$, *Notices Amer. Math. Soc.*, 22(1975), A-485.

[102]William A. Webb, On the diophantine equation $k/n = a_1/x_1 + a_2/x_2 + a_3/x_3$ (loose Russian summary), *Časopis Pěst. Mat.*, 101(1976), 360-365.

[103]H. S. Wilf, Reciprocal bases for the integers, Res. Problem 6, *Bull. Amer. Math. Soc.*, 67(1961), 456.

[104]R. T. Worley, Signed sums of reciprocals Ⅰ, Ⅱ, *J. Australian Math. Soc.*, 21(1976), 410-414, 415-417.

[105]Koichi Yamamoto, On a conjecture of Erdős, *Mem. Fac. Sci. Kyushū Univ.* Ser. A, 18(1964), 166-167; *MR* 30#1968.

[106]K. Yamamoto, On the diophantine equation $4/n = 1/x + 1/y + 1/z$, *Mem. Fac. Sci. Kyushū Univ.* Ser. A, 19(1965), 37-47.

D11. Markoff 方程

一个已吸引了许多人兴趣的丢番图方程是 Markoff 方程

$$x^2 + y^2 + z^2 = 3xyz,$$

它显然有奇异解(1,1,1)和(2,1,1),且所有的解能由这两解产生.因为此方程是每个变量的二次方,因此,一个整数解可导出第二个解,并且能证明,除开奇异解外,所有解有不同的 x,y,z 值.由此知,每一个这样的解恰与另外三个解相邻(图7).1,2,5,13,29,34,89,169,194,233,433,610,985,…被称为 Markoff 数.一个令人瞩目的问题是:图7是个真正的二元树吗?或者两条不同的路径能产生相同的 Markoff 数吗?偶尔有人声称已证明了 Markoff 数只能由一条路径产生,但是,到目前为止的证明都似乎是不可靠的.

如果 $M(N)$ 是满足 $x \leqslant y \leqslant z \leqslant N$ 的三个数的个数.Zagier 已证明 $M(N) = c(\ln N)^2 + O((\ln N)^{1+\epsilon})$,其中 $c \approx 0.180717105$.

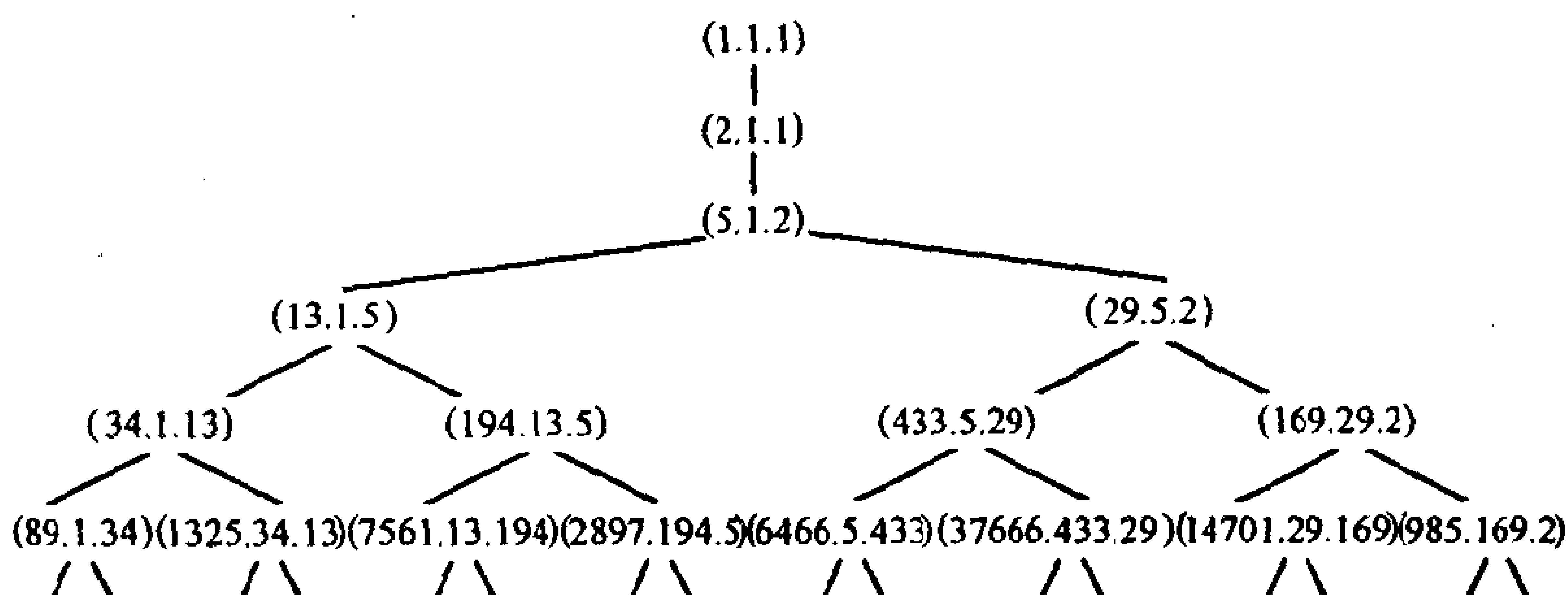


图7 解的 Markoff 链

在大量的计算之后，他猜想 $M(N) = c(\ln(3N))^2 + O((\ln N)^{1/2+\epsilon})$，或者等价地，第 n 个 Markoff 数 m_n 是 $(1/3 + O(n^{-1/4+\epsilon}))A^{\sqrt{n}}$，其中 $A = e^{1/\sqrt{c}} \approx 10.5101504$. Zagier 对这个猜想没有什么结果，但他能证明，此问题与某一类丢番图方程组的不可解性是等价的.

[1]J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge, 1957, 27-44.

[2]H. Cohn, Approach to Markoff's minimal forms through modular functions, *Ann. Math. Princeton*(2)61(1955), 1-12.

[3]T. W. Cusick, The largest gaps in the lower Markoff spectrum, *Duke Math. J.*, 41(1974), 453-463; *MR* 57#5902.

[4]L. E. Dickson, *Studies in the Theory of Numbers*, Chicago Univ. Press, 1930. Chap. Ⅶ.

[5]G. Frobenius, Über die Markoffschen Zahlen, *S.-B. Preuss. Akad. Wiss. Berlin*(1913), 458-487.

[6]A. Markoff, Sur les formes quadratiques binaires indéfinies, *Math. Ann.*, 15(1879), 381-409.

[7]R. Remak, Über indefinite binäre quadratische Minimalformen, *Math. Ann.*, 92(1924), 155-182.

[8]R. Remak, Über die geometrische Darstellung der indefiniten binären quadratischen Minimalformen, *Jber. Deutsch Mato-Verein*, 33(1925), 238-245.

[9]Gerhard Rosenberger, The uniqueness of the Markoff numbers, *Math. Comp.*, 30(1976), 361-365; but see *MR* 53#280.

[10]L. Ja. Vulah, The diophantine equation $p^2+2q^2+3r^3=6pqr$ and the Markoff spectrum (Russian), *Trudy Moskov. Inst. Radiotehn. Elektron. i Avtomat. Vyp.* 67*Mat.*, (1973), 105-112, 152; *MR* 58#21957.

[11]Don B. Zagier, Distribution of Markov numbers, Abstract 796-A37, *Notices Amer. Math. Soc.*, 26(1979), A-543.

D12. 方程 $x^xy^y=z^z$

Erdös 曾猜想，方程

$$x^xy^y=z^z, x>1, y>1, z>1 \qquad (A)$$

没有整数解. 1940年，柯召否定了这个猜想，找到了无穷多个解：

$$x=2^{2^{n+1}(2^n-n-1)+2n}(2^n-1)^{2(2^n-1)},$$

$$y=2^{2^{n+1}(2^n-n-1)}(2^n-1)^{2(2^n-1)+2},$$

$$z=2^{2^{n+1}(2^n-n-1)+n+1}(2^n-1)^{2(2^n-1)+1},$$

这里 $n>1$. 取 $n=2,3,4$ 给出如下解：

x	y	z
12^6	6^8	$2^{11}3^7$
224^{14}	112^{16}	$2^{68}7^{15}$
61440^{30}	30720^{32}	$2^{357}15^{31}$

同时，他证明了$(x,y)=1$时，方程(A)无正整数解. 现在的问题是：柯召找到的正整数解是否是(A)的全部解？1959年，Mills 发现柯召得到的解中 x,y,z 均满足关系 $4xy=z^2$，由此出发，他证明了当 $4xy\geqslant z^2$ 时柯召得到的解是(A)的全部整数解. 1984 年，Uchiyama 证明了当 $4xy<z^2$ 时方程(A)最多只有有限多个整数解. 此外 Schinzel 曾证明，如果方程(A)有整数解，则 x 的每一个

素因子整除 y，或 y 的每一个素因子整数除 x. 并且他猜想，x，y 有相同的素因子. Dem'janenko 证明了这个猜想. 但是方程 $x^x y^y = z^z (1 < x < y)$ 的全部解仍未得到，甚至它是否存在奇数解也没有解决. 从 Mills 与 Uchiyama 的工作很容易让人相信，柯召得到的非平凡解是全部的.

Claude Anderson 猜想，方程 $w^w x^x y^y = z^z$ 没有 $1 < w < x < y$ 的整数解. 但这个猜想是不对的，因为柯召和孙琦早就给出一般方程 $\prod_{i=1}^{k} x_i^{x_i} = z^z (k \geqslant 3, x_i > 1)$ 的无穷多组解（后来还有一些作者给出另外的无穷多组解）. 对 $k = 3$ 的情形，他们给出的解是①

$$x_1 = 3^{A+2n}(3^n - 1)^B, \qquad x_2 = 3^A(3^n - 1)^{B+2},$$

$$x_3 = 3^{A+n}(3^n - 1)^{B+1}, \qquad z = 3^{A+n+1}(3^n - 1)^{B+1},$$

其中 $A = 3^n(3^{n+1} - 2n - 3)$，$B = 2(3^n - 1)$，$n$ 为正整数. 取 $n = 1$ 得 $x_1 = 3^{14}2^4$，$x_2 = 3^{12}2^6$，$x_3 = 3^{13}2^5$，$z = 3^{14}2^5$. 孙琦问，$w^w x^x y^y = z^z (1 < w < x < y)$ 是否有全为奇数的解？曹珍富认为这个问题的回答是肯定的，但没有证明.

[1]V. A. Dem'janenko, On a Canjecture of A. Schinzel, *Inv. Vyss. Vcebn. Zaved. Matematika*, 8(1975), 39-45.

[2]柯召(C. Ko)，孙琦(Q. Sun)，关于方程 $\prod_{i=1}^{k} x_i^{x_i} = z^z$，四川大学学报(自然科学版)，1964，2：5-9.

[3]柯召(Chao Ko)，Note on the diophantine equation $x^x y^y = z^z$，*J. Chinese Math. Soc.*.，2(1940)，205-207；*MR* 2，346.

[4]W. H. Mills, An unsolved diophantine equation, in *Report Inst. Theory of Numbers*, Boulder, Colorado, 1959, 258-268.

[5]A. Schinzel，关于丢番图方程 $x^x y^y = z^z$，四川大学学报(自然科学版)，1958，1，81－83.

[6]孙琦(Q. Sun)，不定方程中的一些结果和问题，自然杂志，8(1985)，5：343

① 注意，[6]中给出的解有误.

—344.

[7]S. Uchiyama, On the Diophantine equation $x^x y^y = z^z$, *Trudy Mat. Inst. Steklov*, 163(1984), 237-243.

D13. 平方数问题

Leo Moser 欲求整数 $a_1, a_2, b_j (1 \leqslant j \leqslant n)$ 使得 $2n$ 个数 $a_i + b_j$ 都是平方数. 这能由使 $a_2 - a_1$ 为一个充足的合数来得到，例如 $a_1 = 0, a_2 = 2^{2n+1}, b_j = (2^{2n-j} - 2^{j-1})^2$.

该问题可推广到 $a_i + b_j$ 是个平方数上，其中 $1 \leqslant i \leqslant m$. 对于 $m = n = 3$，取 $a_i + b_j$ 为下面排列的前三列数的平方，则可找到无穷多组解，

$$\begin{array}{cccc}
\frac{1}{2}(ps+qr) & \frac{1}{2}(qs+rp) & \frac{1}{2}(rs+pq) & \frac{1}{2}(pqr+s) \\
\frac{1}{2}(ps-qr) & \frac{1}{2}(qs-rp) & \frac{1}{2}(rs-pq) & \frac{1}{2}(pqr-s) \\
\frac{1}{4}(p^2+s^2-q^2-r^2) & \frac{1}{4}(q^2+s^2-r^2-p^2) & \frac{1}{4}(r^2+s^2-p^2-q^2) & t
\end{array}$$

其中，为方便计可取 p, q, r, s 为奇. 如果我们包括第四列，则可推广到 $m = 3, n = 4$ 的情形且能找到方程

$$16t^2 = (s^2 - p^2 - q^2 - r^2 + 2)^2 + 4(p^2 - 1)(q^2 - 1)(r^2 - 1)$$

的一个非平凡解. 例如，该方程的一个解由 $q = 2p + 1, r = 2p - 1, t = 2p^3 - p - 1$ 给出，而 s, p 满足 Pell 方程①

$$17s^2 - (17p - 2)^2 = -72$$

(此方程有无穷多组解). 如果 $(s, p) = (21, -5)$ 或 $(219, -53)$，则我们有排列:

$$\begin{array}{cccc}
3^2 & 67^2 & 93^2 & 237^2 \\
102^2 & 122^2 & 138^2 & 258^2 \\
66^2 & 94^2 & 114^2 & 246^2
\end{array}
\quad \text{或} \quad
\begin{array}{cccc}
186^2 & 8662^2 & 8934^2 & 297618^2 \\
11421^2 & 14333^2 & 14499^2 & 297837^2 \\
7074^2 & 11182^2 & 11394^2 & 297702^2
\end{array}$$

对于更大的 n, m 值，情况又如何呢?

① 此方程在 Richard K. Guy 的书(D14)中误为 $17s^2 - (17p - 2)^2 = 72$.

Erdös 和 Leo Moser 又问了类似的问题：对每一个 n，存在 n 个不同的数使得任意一对的和是一个平方数吗？对 $n=3$，我们能取

$$a_1=\frac{1}{2}(q^2+r^2-p^2),a_2=\frac{1}{2}(r^2+p^2-q^2),$$

$$a_3=\frac{1}{2}(p^2+q^2-r^2),$$

且对 $n=4$ 我们可以扩充这些数，例如可取 s 为任意一个能用三种不同的方式表成两平方数和的数，即

$$s=u^2+p^2=v^2+q^2=w^2+r^2$$

和

$$a_4=s-\frac{1}{2}(p^2+q^2-r^2).$$

对 $n=5$，Jean Lagrange 已给出一个相当普遍的参数解和一个简化式，其中简化式给出了所有解中的大部分. 易知，这些解中至多有一个是负的. Jean Lagrange 还把由 J.-L. Nicolas 计算出的头80个解制成表格，最小的是：

$$-4878,4978,6903,12978,31122$$

且最小的正解是

$$7442,28658,148583,177458,763442.$$

他在给 Guy 的一封信(1972年5月19日)中，又给出了 $n=6$ 时的下列解：

$$-15863902,17798783,21126338,$$

$$49064546,82221218,447422978.$$

事实上，T. Baker 找到了5个整数，其成对的和仍是一个平方数. C. Gill 找到5个整数，其三个的和为平方数.

[1]T. Baker, *The Gentleman's Diary*, or *Math. Repository*, London, 1839, 33-5, Quest. 1385.

[2]C. Gill, *Application of the Angular Analysis to Indeterminate Problems*

of Degree 2, N. Y. 1848, p. 60.
[3]Richard K. Guy, *Unsolved Problems in Number Theory*, D14, Springer-Verlag, New York, 1981.
[4]J. Lagrange, Cinq nombres dont les sommes deux à deux sont des carrés, Séminaire Delange-Pisot-Poitou (Théorie des nombres) 12ᵉ année, 20 (1970-71), 10pp.
[5]Jean-Louis Nicolas, 6 nombres dont les sommes deux á deux sont des carrés, *Bull. Soc. Math. France*, Mém No 49-50(1977), 141-143; *MR* 58 #482.
[6]A. W. Thatcher, A prize problem, *Math. Gaz.*, 61(1977), 64.

D14. **Mauldon 问题**

J. G. Mauldon 问，有多少个不同的三个一组的正整数组，其和与积分别是相同的.

对于4个这样的三个一组数集，他说，最小的共同和为118，它来自(14,50,54)，(15,40,63)，(18,30,70)，(21,25,72)，而最小的共同积是25200，它来自(6,56,75)，(7,40,90)，(9,28,100)，(12,20,105). 作为这样原始三个一组数无穷族的一个例子，他给出：$(16ka, bc, 15d)$，$(10ka, 4bc, 6d)$，$(15kb, ad, 16c)$，$(6kb, 4ad, 10c)$，其中 $a = k + 2$，$b = k + 3$，$c = 2k + 7$ 和 $d = 3k + 7$. 他找到5个三个一组数的仅有的例子是(6,480,495)，(11,160,810)，(12,144,825)，(20,81,880)和(33,48,900).

现在还没有6个这样三个一组数的例子，尽管似乎没有理由说明为什么不应有任意大数目的三个一组数.

D15. **Erdös 猜想**

1939年，Erdös 猜想：当 $n > m > 1, k > 2$ 时方程 $\binom{n}{m} = y^k$ 没有正整数解. Erdös 和 Selfridge 已证明，连续整数的积决不是幂，二项式系数 $\binom{n}{m}$ 对于 $n \geq 2m \geq 8$ 决不是幂(此处的幂次数均大于

1). 后者是对 Erdős 猜想的部分回答. 如果 $m=2$，那么 $\binom{n}{2}$ 无穷多次地为一个平方数. 但是，Tijdeman 的方法(见 D8)也许将证明，$\binom{n}{2}$ 决不是一个更高次的幂，且对 $k=3$，除开 $n=50$ 外（见 D3)，它决不给出幂. 曹珍富已经证明了 $\binom{n}{2}$ 决不是一个 $2k$ 次幂($k>1$)，并且他还证明了，1) 在 $n\equiv 0,1 \pmod 4$ 时，$\binom{n}{2}$ 不是一个 k 次幂($k>2$)；2)在 $n\not\equiv 0,2,3,10,11,15,16,23 \pmod{24}$ 时 $\binom{n}{3}$ 不是一个 k 次幂($k>2$). 同时指出，解决 Erdős 猜想将依赖于方程 $x^p+1=2y^p$(p 为奇素数) 的解决. 已知该方程的非零整数解满足 $2\nmid y$ 且 $p\mid(y-1)$. 曹珍富猜想：方程 $x^p+1=2y^p$(p 为奇素数) 无 $|xy|>1$ 的整数解. 徐肇玉用曹珍富的方法(见[4]) 证明了当 $k\geqslant 12\sqrt{2y}$ 时 Erdős 猜想成立.

Erdős 和 Graham 问，是否两个或更多的相邻的连续整数段的积可能是一个幂. Pomerance 已经注意到，如果 $a_1=2^{n-1}$，$a_2=2^n$，$a_3=2^{2n-1}-1$，$a_4=2^{2n}-1$，则 $\prod_{i=1}^{4}(a_i-1)a_i(a_i+1)$ 是一个平方数. 但是，Erdős 和 Graham 认为，如果 $l\geqslant 4$，那么 $\prod_{i=1}^{k}\prod_{j=1}^{l}(a_i+j)$ 仅在有限个场合是平方数.

[1]曹珍富(Z. Cao)，On the diophantine equation $x^{2x}-Dy^2=1$，*Proc. Amer. Math. Soc.*，98(1986)，11-16；*MR* 87*i*：11035；*Zbl*. 596. 10016.

[2]曹珍富(Z. Cao)，An Erdős conjecture，Pell sequence and Diophantine equation，*J. Harbin Inst. Tech.*，1987，2：122-124；*MR* 89b；11022.

[3]曹珍富(Z. Cao)，关于丢番图方程 $x^p-y^p=Dz^2$，东北数学，2(1986)，2：219－227；*MR* 88b：11013.

[4]曹珍富(Z. Cao)，丢番图方程引论，哈尔滨工业大学出版社，1989，126页；*MR* 92e：11018.

[5]P. Erdős，On a diophantine equation，*J. London Math. Soc.*，26(1951)，

176-178.
[6]P. Erdős, on consecutive integers, *Nieuw Arch. Wisk.*, 3(1955), 124-128.
[7]P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.*, 19(1975), 292-301.
[8]徐肇玉(Z. Xu),关于 Erdős 猜想,自然杂志,14(1991),2:158－159.

D16. 有理距离问题

是否存在一个点,它到单位正方形各顶角的距离都为有理数?早些时候,人们认为没有三个这样有理距离的非平凡例子(即不是在正方形的一边上). 但是,John Conway 和 Mike Guy 找到了方程

$$(s^2+b^2-a^2)^2+(s^2+b^2-c^2)^2=(2bs)^2$$

的无穷多个解,其中 a,b,c 是某一点到边长为 s 的正方形三个顶点的距离. 图8给出了这样的解能够得到两个三距离问题的解.

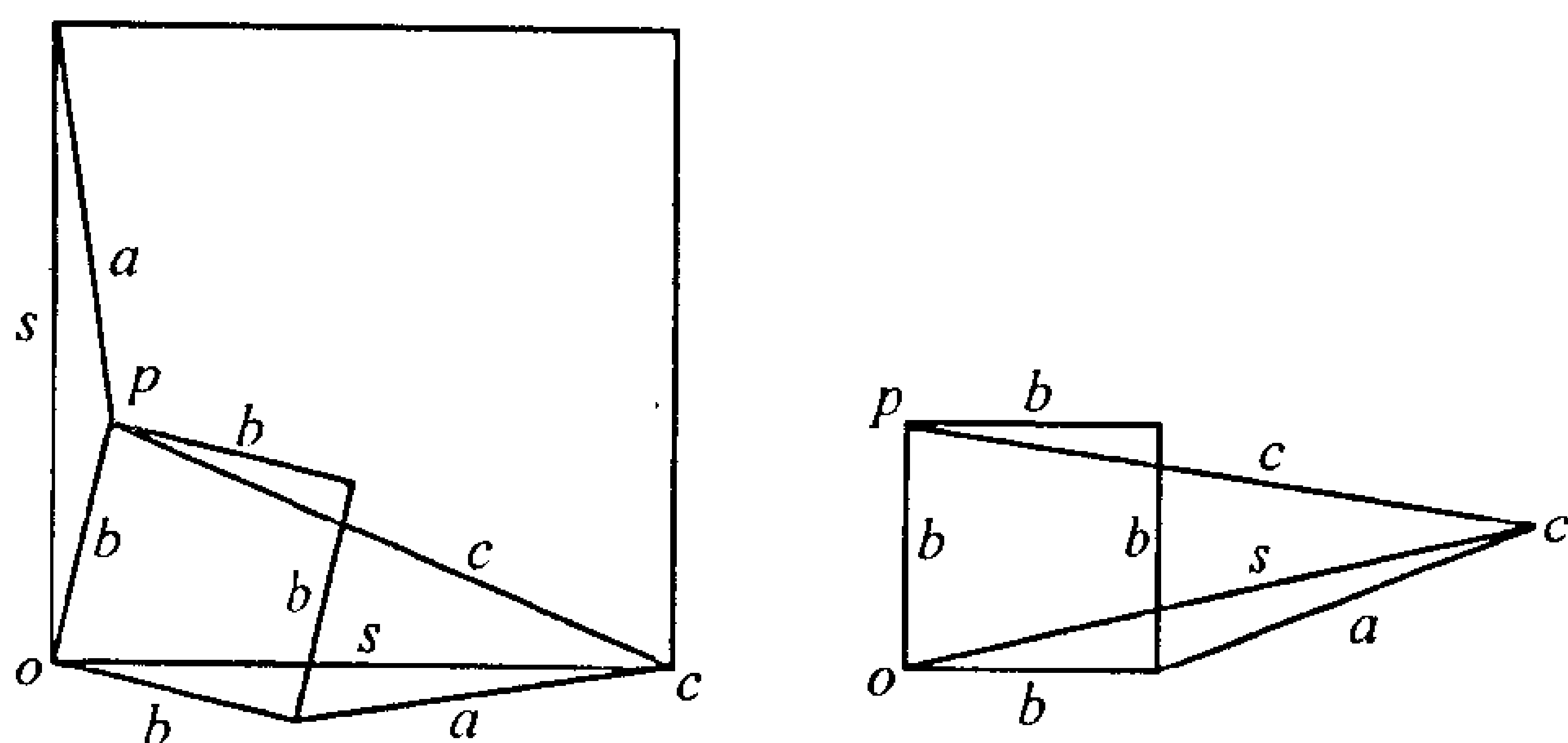


图8　两相关的三距离问题解

当第四个距离也是整数时,我们又要求 $a^2+c^2=b^2+d^2$. 在三距离问题中,s,a,b,c 一个被 3 除尽,一个被 4 除尽,且一个被 5 除尽. 在四距离问题中,s 是 4 的倍数,a,b,c,d 为奇(假定它们不存在公因子). 如果 s 不是 3(或 5) 的倍数,那么 a,b,c,d 中的两个被 3(或 5) 除尽.

在距一个边为 t 的等边三角形的顶点距离 $a,b,c(a,b,c$ 都为整数) 的对应问题中,有无穷多个解. 在这些解中,a,b,c,t 中的一

个被 3、一个被 5、一个被 7 和最后一个被 8 除尽.

Jerry Bergum 问,对什么样的整数 n,存在正整数 x,y,其中 $(x,y)=1$,x 为偶,使得 $x^2+y^2=b^2$ 和 $x^2+(y-nx)^2=c^2$ 都为完全平方数.如果 $n=2m(2m^2+1)$,那么 $x=4m(4m^2+1)$,$y=mx+1$ 是一个解.对于 $n=\pm 1$, ± 2, ± 3,或 ± 4,没有解存在.如果 $n=8$,y 存在时,最小的 x 是 $x=2996760=2^3\times 3\times 5\times 13\times 17\times 113$.此问题与原问题联系是:$(x,y)$ 都是 P 点的坐标.P 点离原点 O 的距离为 b,离边长 $s=nx$ 的正方形的邻角 C 的距离为 c,其中 n 为整数.

Ron Evans 注意到,问题可这样来陈述:在整数边的三角形中,其底与高之比是哪一个整数?n 的符号随三角是锐(钝)角而正(负)变化(例如 $n=-29$,$x=120$,$y=119$ 是一个解).他也问了一个孪生问题:试找到每一个整数边的三角形,其底除尽它的高.这里,(高/底)不可能是1,2,但可能是3(例如,底为4,边为13,15,高为12).

[1]R. B. Eggleton, Tiling the plane with triangles, *Discrete Math.*, 7(1974), 53-65.

[2]R. B. Eggleton, Where do all the triangles go? *Amer. Math. Monthly*, 82(1975), 499-501.

[3]Ronald Evans, Problem E2685, *Amer. Math. Monthly*, 84(1977), 820.

[4]N. J. Fine, On rational triangles, *Amer. Math. Monthly*, 83(1976), 517-521.

[5]J. G. Mauldon, An impossible triangle, *Amer. Math. Monthly*, 86(1979), 785-786.

[6]C. Pomerance, On a tiling problem of R. B. Eggleton, *Discrete Math.*, 18(1977), 63-70.

D17. 有理距离的6个点问题

是否存在这样的平面上6个点,它们没有三点共线,没有4点共

圆,其所有点的相互距离为有理数.已知有可数的不共线且相互距离为有理数的无穷多个点存在,但是,除了两个点以外,其余的均在一个圆上.

有两个相互对立的猜想:(*a*)存在数 c 使得其相互距离为有理数的 n 个点必定包含至少 $n-c$ 个点在一个圆或一条直线上;(*b*) Besicoritch 猜想:任意多边形都被一有理多边形来进行任意程度的近似.

如果我们放宽条件,比如说,至多4点共线,至多4点共圆,则 John Leech 找到了如图9 (*a*) 所示类型的 7 个点的无穷多个集合和如图 9(*b*) 所示的8个点的无穷多个集合.他说,后者情形似乎是由于解"太多"的方程而造成的数字畸形(关于三个同类变元的4个方程).

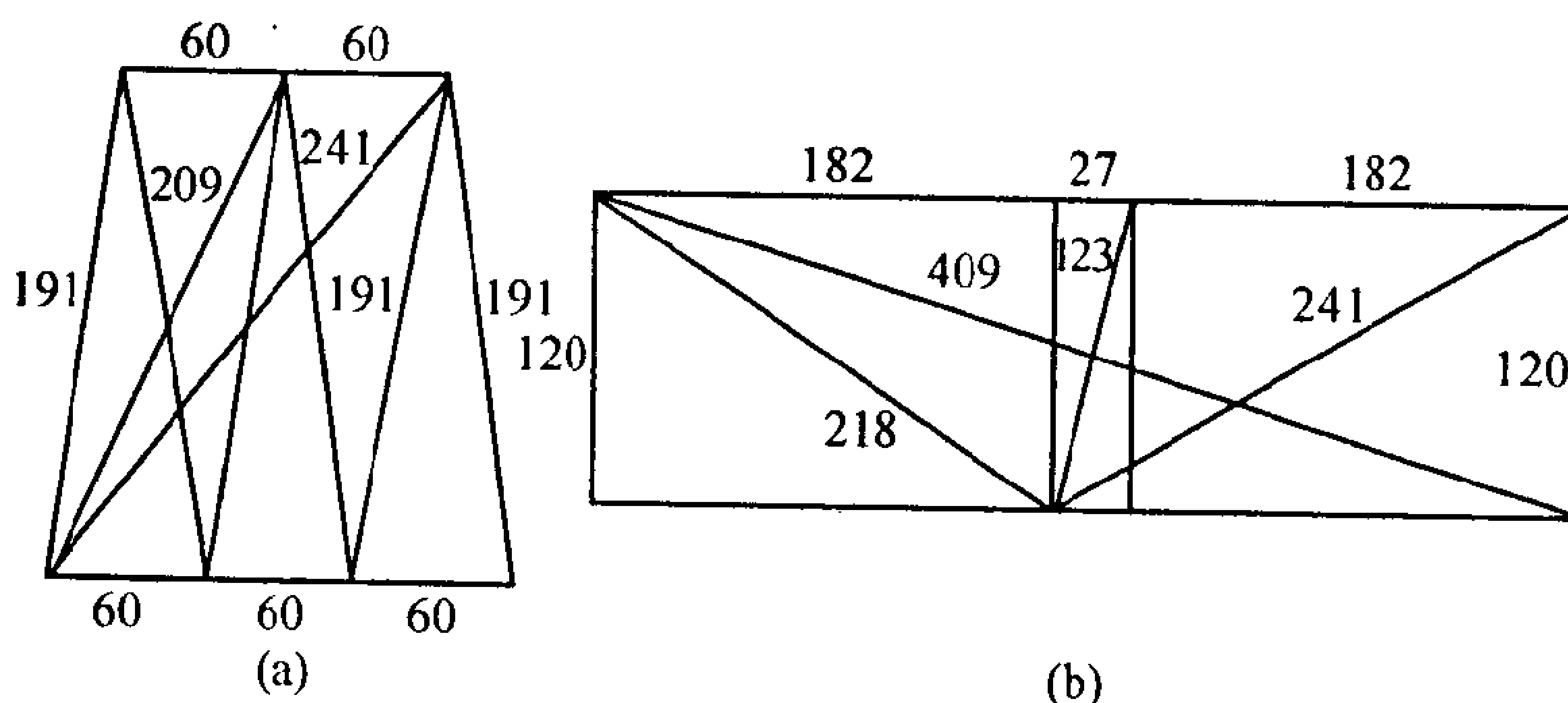


图9 Leech 的有理距离的点的构型

[1]J. H. J. Almering, Rational quadrilaterals, *Nederl. Akad. Wetensch. Proc. Ser.* A66 = *Indag. Math.*, 25(1963), 192-199; Ⅱ *ibid*, 68 = 27(1965), 290-304; *MR* 26#4963, 31#3375.

[2]D. D. Ang, D. E. Daykin and T. K. Sheng, On Schoenberg's rational polygon problem, *J. Austral. Math. Soc.*, 9(1969), 337-344; *MR* 39#6816.

[3] A. S. Besicovitch, Rational polygons, *Mathematika*, 6(1959), 98; *MR*22#1557.

[4] D. E. Daykin, Rational polygons, *Mathematika*, 10(1963), 125-131; *MR*30#63.

[5] D. E. Daykin, Rational triangles and parallelograms, *Math. Mag.*, 38(1965), 46-47.

[6] L. J. Mordell, Rational quadrilaterals, *J. London Math. Soc.*, 35(1960), 277-282.

[7] T. K. Sheng, Rational polygons, *J. Austral. Math. Soc.*, 6(1966), 452-459; *MR* 35#137.

[8] T. K. Sheng and D. E. Daykin, On approximating polygons by rational polygons, *Math. Mag.*, 38(1966), 299-300; *MR* 34#7463.

D18. 三角形问题

存在一个三角形，其边、中线、面积均为整数吗?在文献中有一个否定性“证明”是不正确的，因此此问题仍然悬而未决.

我们知道，具有整数边的三角形，如果面积也为整数，那么称之为 Heron 三角形. 有一个众所周知的问题是:Heron 三角形的三条边长能否都取 Fibonacci 数(见 A3)?这样的三角形如果存在，就称之为 Fibonacci 三角形. 易知，Fibonacci 三角形的边长只可能是 (F_{n-1}, F_{n-1}, F_n) $(n \geqslant 4)$，或 (F_{n-k}, F_n, F_n) $(1 \leqslant k < n)$，前者易知仅当 $n = 6$，$(F_5, F_5, F_6) = (5, 5, 8)$ 构成 Fibonacci 三角形. 对后者，Harborth 与 Kemnitz 证明了 $k = 1$ 或 $n \leqslant 25$ 时不存在边长为 (F_{n-k}, F_n, F_n) $(1 \leqslant k < n)$ 的 Fibonacci 三角形. 曹珍富给出研究 Fibonacci 三角形的一般方法，用此方法可证明 $k = 2, 3, 4$时这种三角形均是不存在的. 一般的看法是:当 $1 \leqslant k < n$ 时，不存在以 (F_{n-k}, F_n, F_n) 为边长的 Fibonacci 三角形.

存在一个任意维数的单纯形，其长度、面积、体积、超体积均为有理数吗?两维时，回答是肯定的，有无穷多个 Heron 三角形，其边和面积均为有理数. 一个例子是边为13，14，15，面积为84的三角形. 在三维时，答案也是肯定的. 那么所有的四面体都能由有理四面体来进行任意程度的近似吗?

[1]陈计(Z. Chen)编译,斐波那契三角形,数学通讯,1994,5:41.
[2]H. Harborth and A. Kemnitz, Fibonacci triangles, *Applications of Fibonacci Numbers*, Vol. 3(Pisa,1988),129-132,Kluwer Acad. Publ. Dordrecht,1990; *MR* 92f:11025.
[3]Richard K. Guy, *Unsolved Problems in Number Theory*, D21,Springer-Verlag,New York,1981.

D19. 方程$(x^2-1)(y^2-1)=(z^2-1)^2$

另一个未解决的丢番图方程是

$$(A)\qquad (x^2-1)(y^2-1)=(z^2-1)^2.$$

已知Schinzel和Sierpinski对于$x-y=2z$的情形,找到了全部解;曹珍富和王彦斌已找到其他情形的解,例如给出了$1\leqslant|l|\leqslant 30$,$x-y=lz$情形的全部解.也对$l\in Z$,$|l|\neq 2$时作了不存在非平凡解的猜想.曹珍富注意到Schinzel与Sierpinski考虑的情形是方程$xy=z^2+2$,$x-y=2z$,因而研究了一般的联立方程$axy=bz^2+c$与$dx-ey=fz$的公解.由此得出了方程$(ax^2+db^2)(ay^2+dc^2)=(ez^2+f)^2$的一系列结果,包含了Mordell的书中总结的Szymiczek等人的相应研究.1996年,Luca证明了上述猜想成立,并且他进一步地给出了满足$z\mid(y^2-x^2)$的(A)的全部解.

此外,1987年曹珍富问,方程$(x^4-1)(y^4-1)=z^2(x^2\neq 1, y^2\neq 1)$的解如何?从方程$x^4-Dy^2=1$的结果可推出它最多有一组$x^2>y^2$的解(参阅D5),且在$(x^4-1,y^4-1)>\exp 64$时无$x^2>y^2$的解.我们希望用完全初等的方法证明该方程仅有$x^2>y^2$的解$(x^2,y^2)=(239^2,13^2)$.

[1]曹珍富(Z. Cao),关于Schinzel-Sierpinski方程组的推广,哈尔滨工业大学学报,23(1991),5:9—14; *MR* 93b:11026.
[2]曹珍富(Z. Cao),数论中的几个未解决问题,哈尔滨师专学报,1987,4:14—18.
[3]F. Luca, A generalization of the Schinzel-Sierpinski system of equation, September 21,1996 (to appear).

[4]L. J. Mordell, *Diophantine equations*, Academic Press, New York, 1969, 97.

[5]A. Schinzel and W. Sierpinski, Sur l'equation diophantienne $(x^2-1)(y^2-1)=[((y-x)/2)^2-1]^2$, *Elem. Math.*, 18(1963), 132-133; *MR* 29#1180.

D20. 和等于积问题

对于 $k>2$，方程 $a_1a_2\cdots a_k=a_1+a_2+\cdots+a_k$ 总有正整数解 $a_1=2, a_2=k, a_3=a_4=\cdots=a_k=1$（即 k 个正整数中有一个为 2，一个为 k，其余均为 1，这种情形称为方程的一个解）. 现在的问题是：对哪些 k，方程恰有一个解？Schinzel 证明了在 $k=6$ 或 $k=24$ 时不存在另外的解. Misiurewicz 已证明：当 $2<k<1000$ 时，$k=3,4,6,24,144,174$，和 444 是使方程恰有一个解的情形. 曹珍富发现，$k=144$ 的情形是错误的，例如此时有另外的解 $a_1=12, a_2=14, a_3=\cdots=a_{144}=1$ 以及 $a_1=2, a_2=4, a_3=21, a_4=\cdots=a_{144}=1$. 事实上，取 $a_4=\cdots=a_k=1$，则方程化为 $a_1a_2a_3=a_1+a_2+a_3+k-3$，当 $a_3=1$ 时得出 $(a_1-1)(a_2-1)=k-1$；当 $a_1=2$ 时得出 $(2a_2-1)(2a_3-1)=2k-1$. 由此知，方程恰有一个解的必要条件是 $k-1$ 与 $2k-1$ 均为素数（$k=144$ 时 $k-1=11\times 13, 2k-1=7\times 14$）. 曹珍富问：是否存在无穷多个 k，使方程恰有一个解？仅有有限个吗？

[1]Richard K. Guy, *Unsolved Problems in Number Theory*, D24, Springer-Verlag, New York, 1981.

[2]M. Misiurewicz, Ungelöste Probleme, *Elem. Math.*, 21(1966), 90.

D21. 与 $n!$ 有关的方程

方程 $n!+1=x^2$ 仅有解 $n=4,5,7$ 吗？Erdös 和 Obláth 解决了 $n!=x^p\pm y^p$，且 $(x,y)=1, p>2$ 的情形，但 $p=2$ 的情形未能解决.

Simmons 注意到 $n!=(m-1)m(m+1)$ 有正整数解 (m,n)

$=(2,3),(3,4),(5,5)$和$(9,6)$，并问：是否还有其他的正整数解？

[1]H. Brocard, Question 1532, *Nouv. Corresp. Math.*, 2(1876), 287; *Nouv. Ann. Math.*, (3)4(1885), 391.

[2]P. Erdös and R. Obláth, Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$, *Acta Szeged*, 8(1937), 241-255.

[3]M. Kraitchik, Recherches sur la Theorie des Nombres, t. 1, Gauthier-Villars, Paris, 1924, 38—41.

[4]Richard M. Pollack and Harold N. Shapiro, The next to last case of a factorial diophantine equation, *Comm. Pure Appl. Math.*, 26(1973), 313-325; *MR* 50#12915.

[5]G. J. Simmons, A factorial conjecture, *J. Recreational Math.*, 1(1968), 38.

D22. Fibonacci 数问题

Stark 问，哪个 Fibonacci 数(见 A3)是两个立方数的差(或和)的一半？这与寻找全部类数2的复合二次域的问题有关. 例子有：$1=\frac{1}{2}(1^3+1^3), 8=\frac{1}{2}(2^3+2^3), 13=\frac{1}{2}(3^3-1^3)$.

Vern Hoggatt 问，是否1,3,21和55是仅有的为三角形数(即形如$\frac{1}{2}m(m+1)$)的 Fibonacci 数？罗明用递推序列方法给出了这个问题的肯定回答，但证明非常麻烦. 是否有一个非常简洁且初等的证明？关于 Fibonacci 数表平方数或2倍的平方数问题已由 Cohn 解决.

[1]J. H. E. Cohn, On Square Fibonacci Numbers, *J. London Math. Soc.*, 39(1964), 537-541.

[2]罗明(M. Luo), On triangular Fibonacci numbers, *The Fibonacci Quarterly*, 27(1989), 2: 98-108.

[3]H. M. Stark, Problem 23, *Summer Institute on Number Theory*, Stony Brook, 1969.

D23. 同余数问题

同余数与 Pythagorean 三角形(即直角三角形)有关,已有相当长的历史了. 早在一千多年前,阿拉伯人的手稿中就已给出了几个例子(5,6,14,下页表7中的17项 CA,以及10个大于1000的同余数). 另一方面,它至今仍吸引着许多人的兴趣. 所谓同余数是指使联立方程

$$x^2+ay^2=z^2, x^2-ay^2=t^2$$

有正整数解的那些整数 a. 也许,它的魅力便在于最小解的大小常常是不规则的. 例如,$a=101$ 是同余数,Bastien 给出了最小解

$$x=2015242462949760001961, y=118171431852779451900$$
$$z=2339148435306225006961, t=1628124370727269996961.$$

等价地,同余数是那些 a,它使丢番图方程

$$x^4-a^2y^4=u^2$$

有正整数解. Dickson 的《数论的历史》(*History of the Theory of Numbers*, Chelsea Publishing company, New York, 1952)一书给出了许多早期的参考文献,它包括 Pisa(Fibonacci)的 Leonardo; Genocchi; 和 Gerardin. 他们给出了7,22,41,69,77以及表7中20个阿拉伯人的例子及43项 CG. 显然,我们仅需考虑 a 为无平方因子就够了. 因为如果 $b=ad^2$,那么,关于 a 的方程的解(x,y,z,t)便与关于 b 的方程的解(dx,y,dz,dt)相对应了.

人们猜想,无平方因子数≡5,6或7(mod 8)是同余的. Nelson Stephens 证明了此猜想的成立取决于 Selmer 对椭圆曲线的猜想(见 Cassels 的文献). 因此,从 Heegner 的工作(见 Birch 的文献)知,这对素数≡5,或7(mod 8)和素数≡3(mod8)的2倍成立. 这些便是表7中 C5,C7和 C6项. Bastien 注意到下列数是非同余的:素数≡3(mod 8),以及两个这样的素数积;素数≡5(mod8)的2倍,以及两上这样的素数积的倍数;素数≡9(mod16)的2倍. 这些是表7中的 N3,N9,NX(对10=2×5),NL(对50=2×5×5)和 N2项. 他还给出了其它一些非同余数(表7中的 NB),并且得到:如果 a 是素

表7. 已知的小于1000的同余数(C)和非余数(N)

$a = 40c + r$ 的项在 c 列,r 行.

r \ c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	NB	C1	□	□	CG	N9	N1	N1	N9	□	N1	□	NJ	N1	CG	N1	N1	N9	C&	C1	□	□	1	N9	□
2	NB	NB	N2	NX	□	NX	□		NJ	NX	NJ	CG		□	N2	CG	NJ	NJ	□	NJ		NX	□	NX	NL
3	NJ	N3	N3	N&	N3	NJ	□	N3	C&	□	N.		NJ	N3	N3	□	N3	N3	CJ	NJ	NJ	NJ	N3	NJ	□
4	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
5	C5	□	CG	□	CG	CG	□	C&	□	CJ	□	C&	CJ	□	C&	□	C&	CJ	□	□	C&	□	CJ	□	
6	C6	C6	C6	□	C6	C6	C&	CA	C6	C&	CJ	C6	□	C6	C6	CJ	CG	□	□	C6	CG	□	C6	C6	CG
7	C7	C7	CG	C7	C7	□	CJ	C&	CJ	C7	CJ	CJ	C7	C&	□	C7	C7	CJ	C7	CJ	CJ	□	C7	□	C7
8	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
9	□	□	N1	N9	□	N9	N9	□	NJ	□	N1	N1	N9	□	1	C&	N9	C&	□	N1	1	N9	C&	N1	NJ
10	NX	□	□	NL	N&	CA	□	NL	CA	NL	CG	□	□	NL	NJ	NL	□	NJ	NJ	NJ	□	□	CG	NJ	NJ
11	N3	NB	NB	N3	□	N1	NJ	CG	N3	CG	NJ	NJ	N3	□	NJ	NJ	CG	NJ	C&	NJ	N3	NJ	□	□	N3
12	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
13	C5	C5	CG	CJ	C5	CJ	CJ	C5	□	C5	CJ	CJ	CJ	C&		C5	C5	□	C5	C5	C&	C5			CJ
14	C6	□	C6	C6	CG	C6	C6	□	C6	CJ	□	C6	CJ	CJ	C&	C6	CJ	C6	C6	□	C&	CJ	CJ	C6	C&
15	CA	CG	CG	□	□	C&	CG	CJ	CJ	□	CJ	C&	□	C&	□	C&	CJ	CJ	□	□	CJ	□	CJ	C&	□
16	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
17	N1	N9	N1	C1	N9	NJ	C1	□	N1	NJ	N9	C1	NJ	N9	1	N1	□	NJ	N9	C&	N9	1		N1	N1
18	□	NX	□	CG	N2	NX	NJ	NX	□	□	NJ	NX	NJ	NX	□	NJ	C&	NX	□	NX	N2	NJ			NJ
19	N3	N3	□	N3	N3	C&	NJ	CG	NJ	N3	N3	□	N3	□	NJ	N3	N3	NJ	N3	NJ	□	N3	NJ		NJ
20	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
21	CA	C5	C5	C&	C5	CA	□	CJ	CJ	CJ	C5	C5	CJ	C5	CJ	□	C5	C5	CG	CJ	C5	CJ	C&	C5	□
22	C6	C6	CG	C6	C&	CJ	C6	C6	□	C6	C6	CG	C6	C6	C&	C6	C6	□	CJ	CJ	CJ	C6	CJ	CJ	C6
23	C7	□	C7	C&	CJ	C7	C7	□	□	C7	□	C7	C7		CG		C&	CJ	C7	□	C7	C7	C&	C&	C7
24	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
25	□	CA	NJ	CG	NJ	□	CG	NJ	NJ	NJ	□	CG	C&	NJ	□	□	NJ	NJ	NJ	NJ	□	NJ	C&	□	C&
26	NX	NB	NX	N2	N&	C&	NJ	□	NX	C&	C&	N2	NJ	CA	NX	N2	□		NX	NJ	NJ	C&	NJ	NJ	NJ
27	□	N3	N3	□	N&	N3	NJ	N3	N3	□	NJ	N3	□	N3	N3		NJ	NJ	□	N3	N3	□	N3	NJ	C&
28	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
29	C5	CG	C5	C5	□	C5	C5	CJ	C5	C5	CA	CJ	C5	□	CJ	C&	C&	C5	CJ	CJ	C5	CJ	□	C&	CJ
30	CA	CA	CA	□	CA	CJ	□	CG	□	CA	CJ	CG	CG	□	CJ	□	C&	C&	□	CJ	CJ	C&	C&	□	□
31	C7	C7	CG	C7	C7	CA	C7	C7	□	C&	C7	CJ	C&	CJ	CJ	C7	C&	□	C7	C&	CJ	CJ	C7	C&	C7
32	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
33	N9	N1	N1	□	N1	N1	NJ	C1	C1	N9	N1	N9	□	NJ	1	N9	N1	NJ	N9	C&	□	□	N9	1	N9
34	CA	NX	N&	CA	C&	□	N2	NX	NJ	NX	CG	NJ	C&	NX	□	NX	C&	NJ	NL	NX	NJ	NJ	N2	□	NJ
35	NB	□	N&	NJ	NJ	NJ	□	□	NJ	C&	NJ	□	NJ	NJ	NJ	NJ	□	NJ	NJ	NJ	NJ	□	C&	NJ	C&
36	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
37	C5	CG	□	C5	C5	CJ	C5	C5	CG	C5	CJ	□	CG	C5		□	C5		C5	C5	□	C5		C&	C5
38	C6	CG	C6	C6	□	CJ	C6	C&	C6	C6	CG	C6	C&	□	CJ	CJ	CJ	C6	C6	CG	C6	C6	□	C6	C6
39	CG	C7	C&	C&	C7	C7	□	C&	C7	C&	C7	C7	CJ	CJ	C7	□	CJ	C7	CG	C&	C7	C&	C7	C&	□
40	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

数≡1(mod8),且 $a = b^2 + c^2$ 和 $b + c$ 是 a 的二次非剩余(见F5),则 a 是非同余的. 这也解释了几个N1情况. 因此,此表也可作为<1000的素数表,那些≡1(mod 8)的数也都已在表7中示出(由C1,N1或状况未明时用1). C& 和 N& 项来源于 Alter 等人,CJ 和 NJ 项来自于 Jean Lagrange 的大量论文. 方框(□)表明该数含有重复因子,空白表示状态不明.

我们很难保证上面收集到的是全部的结果,因为其中许多(特

别是由构造性得到的）总是不发表的. 应该非常感谢 J. A. H. Hunter，他已获得或是激发了下面几项的构造. M. R. Buckley 和 K. Gallyas（Fibonacci Assoc. Newsletter，Sept. 1975）找到了

$$1341306649380472283747020010796 97^2 \pm 103 \times 7188661768365914788447417161240^2$$

两者均为平方数，而 Hunter 和 Buckley 找到最小表示

$$7646464402119589982672 41^2 \pm 229 \times 940450645748978061318 0^2$$

$$7777776188475562106450 41^2 \text{ 或 } 7512857862873937986494 41^2$$

和

$$407893921^2 \pm 239 \times 4826640^2 = 414662879^2 \text{ 或 } 401010721^2.$$

作为远比103情形大的例子，Hunter 给出了补充算式

$$49143127346631084^2 \pm 46867792486220437^2$$

$$= 67909034288072605^2 \text{ 或 } 263 \times 911391767518393^2.$$

对于已知的小于1000中的221个同余数，他得到 (x,y)，如 $5829043537^2 \pm 457 \times 234834600^2 = 7692857713^2$ 或 2962336463^2，而同时 $86236037017^2 \pm 133 \times 7049242860^2$ 和 $318957135928681^2 \pm 183 \times 7531376243820^2$ 都是平方数，但是仍然有一百多个数，其解仍未能构造出来.

Jean Lagrange 在给 R. K. Guy 的一封信中注意到，尽管897出现在 Gérardin 的表中，但是其角色仍然未知，因此我们把它从表7中拿掉了. 他也报造说，他已证明，113，337，409和521是非同余的，且希望能够将≡1，2或3(mod 8)的那些数分类. 下面是表7的一个总结：

模8剩余类	1	2	3	5	6	7	总数
已知的同余数	22	19	12	95	103	101	352
已知的非同余数	68	76	87	0	0	0	231
状况不明的总数	8	6	2	7	0	2	25
无平方因子数的总数	98	101	101	102	103	103	608

[1]Ronald Alter, The congruent number problem, *Amer. Math. Monthly*, 87(1980), 43-45.

[2]R. Alter and T. B. Curtz, A note on congruent numbers, *Math. Comp.*, 28(1974), 303-305; *MR* 49#2504.

[3]R. Alter, T. B. Curtz and K. K. Kubota, Remarks and results on congruent numbers, *Congressus Numerantium* Ⅶ, *Proc. 3rd S. E. Conf. Combin. Graph Theory*, Comput. 1972, 27-35; *MR* 50#2047.

[4]L. Bastien, Nombres congruents, *Intermédiaire des Math.*, 22(1915), 231-232.

[5]B. J. Birch, Diophantine analysis and modular functions, *Proc. Bombay Colloq. Alg. Geom.*, 1968.

[6]J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.*, 41(1966), 193-291.

[7]L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Diophantine Analysis, Washington, 1920, 459-472.

[8]A. Genocchi, Note analitiche sopra Tre Seritti, *Annali di Sc. Mat. e Fis.*, 6(1855), 273-317.

[9]A. Gérardin, Nombres congruents, *Intermédiaire des Math.*, 22(1915), 52-53.

[10]H. J. Godwin, A note on congruent numbers, *Math. Comp.*, 32(1978), 293-295 and 33(1979), 847; *MR* 58#495; 80c:10018.

[11]Richard K. Guy, *Unsolved Problems in Number Theory*, D27, Springer-Verlag, New York, 1981.

[12]Jean Lagrange, Thèse d'Etat de l'Université de Reims, 1976.

[13]Jean Lagrange, Construction d'une table de nombres congruents, *Bull. Soc. Math. France Mém.*, *No.* 49-50(1977), 125-130; *MR* 58#5498.

[14]L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969, 71-72.

[15]S. Roberts, Note on a problem of Fibonacci's, *Proc. London Math. Soc.*, 11(1879-80), 35-44.

[16]N. M. Stephens, Congruence properties of congruent numbers, *Bull. London Math. Soc.*, 7(1975), 182-184; *MR* 53#260.

D24. 方程$\frac{1}{w}+\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{wxyz}=0$

Mordell 问:方程

$$(A)\qquad \frac{1}{w}+\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{wxyz}=0$$

的解如何?1984年,曹珍富给出了这个方程的全部整数解.但解的参数满足一些条件,如方程

$$\frac{1}{x}=\frac{1}{y_1}+\frac{1}{z_1}+\frac{1}{w_1}+\frac{1}{xy_1z_1w_1}$$

的全部正整数解可表为

$$x=n, y_1=n+k, z_1=n+(n^2+t)/k,$$
$$w_1=[n(n+k)(n+(n^2+t)/k)+1]/t,$$

这里正整数 n,k,t 满足

1) $n^2+t\equiv 0(\bmod k)$;

2) $n(n+k)(n+\frac{n^2+t}{k})+1\equiv 0(\bmod t)$;

3) $(n,k)=(k,t)=(n,t)=1$.

在 $2\nmid n$ 或 $2\nmid k$ 时,可证满足 1)～3) 的 n,k,t 有如下的关系:$k\equiv t\equiv 1(\bmod 4)$ 且 Jacobi 符号 $\left(\frac{k}{t}\right)=1$. 由此容易构造方程当参数 $k>1,t>1$ 的某些解,例如取 $t=5,k=41$,由 1)～2) 解出 $n\equiv 6, 88, 158(\bmod 205)$,以 $n=205n_1+6$ 为例代入上述解中得

$$x=205n_1+6, y_1=205n_1+47, z_1=1025n_1^2+265n_1+7,$$
$$w_1=8615125n_1^4+4454650n_1^3+692490n_1^2+30157n_1+395.$$

我希望由1)～3)给出一般地容易构造方程 (A) 解的其他条件来.

对于方程

$$(B)\qquad \frac{1}{x_1}+\cdots+\frac{1}{x_s}+\frac{1}{nx_1\cdots x_s}=\frac{1}{n}, 1<x_1<\cdots<x_s,$$

设 $\Omega_n(s)$ 表示其解的个数,曹珍富与田红旗证明了:当 $n\equiv 7, 18, 22(\bmod 25)$ 且 $s\geqslant 3$时,

$$(C)\qquad 0<\Omega_n(s)<\Omega_n(s+1).$$

对于另外的某些 n，也能证明(C)成立．但我不知道是否对所有的 n，(C)均成立(当 $s\geq 4$ 时)．这个问题的肯定回答将导致另一个问题(见 F30)的解决．

[1]曹珍富(Z. Cao)，数论中的几个未解决问题，哈尔滨师专学报，1987，4:11－18.

[2]曹珍富(Z. Cao)，关于单位分数的 Mordell 问题，数学杂志，7(1987)，3:245－250; *MR* 90a:11032.

[3]曹珍富(Z. Cao)，，数论中的一些新的问题和结果，河池师专学报，1987，1:1－8.

[4]曹珍富(Z. Cao)，丢番图方程引论，哈尔滨工业大学出版社，1989; *MR* 92e:11018.

[5]曹珍富(Z. Cao)，田红旗(H. Tian)，关于丢番图方程 $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{nx_1\cdots x_s}=\frac{1}{n}$，《青年科技论文集》，黑龙江科技出版社，1990，7－11.

[6]L. J. Mordell, Research Problem 6, *Canad. Math. Bull.*, 17(1974), 141.

D25. 公解问题与某些二元高次方程

利用 Baker 的方法可知，给定 D_1, D, k 和 l，方程 $x^2-Dy^2=k$ 和 $y^2-D_1z^2=l$ 仅有有限组解(可以定出解的绝对值的上界)．是否可以给出最多只有几个解的结论?曹珍富猜想：

Pell 方程 $x^2-Dy^2=1$ 和 $y^2-D_1z^2=1$ 最多只有一组正整数的公解．

曹珍富对于方程 $x^{2n}-Dy^2=1(n>2)$ 已有过不少工作，例如他证明了：设 Pell 方程 $u^2-Dv^2=-1$ 有整数解，则方程 $x^{2n}-Dy^2=1(n>2)$ 除开 $n=5, D=122, x=3, y=22$ 外，无其他的正整数解．他猜想：方程 $x^{2n}-Dy^2=1(n>2)$ 最多只有一组正整数解，且设 Pell 方程 $\xi^2-D\eta^2=1$ 的基本解为 ϵ，则有 $x^n+y\sqrt{D}=\epsilon$．这个猜想的证明将需要首先解决方程 $x^p+1=2y^2$(p 为奇素数)的求解问题，已知这个方程的正整数解除 $x=y=1$ 外满足 $2p\mid y$．

1987年，曹珍富又猜想：方程 $x^p+1=2y^2$ 在素数 $p>3$ 时仅有正整数解 $x=y=1$. 1989 年，乐茂华用 Baker 方法证明：当 $p>2^{2415}$ 时这一猜想是正确的.

在研究一类实二次域类数的可除性时，曹珍富证明了：当方程 $u^2-Dv^2=4,(u,v)=1$ 有整数解时，方程 $4x^{2n}-Dy^2=-1$ $(n>2)$ 仅有正整数解：$D=5,x=y=1$. 他与 Nagell 使用不同的方法分别给出了 $x^p-1=2y^2$（p 是奇素数）的全部正整数解：$p=5,x=3,y=11$. 对于一般的方程

(A) $$x^p\pm 1=Dy^2,xy\neq 0,$$

当 $D>0$ 无平方因子，且不被 $2mp+1$ 形素数整除，p 是大于 3 的奇素数时，曹珍富证明了除 $1^p+1=2(\pm 1)^2$ 和 $3^5-1=2(\pm 11)^2$ 外，方程 的整数解均满足 $2p|y$. 由此可以推出柯召关于 Catalan 猜想(D8)的著名定理，以及方程 $x^{2p}-Dy^2=-1$（p 是奇素数，D 的条件同前）仅有正整数解 $D=2,x=y=1$. Nagell 对于 (A) 中取减号的方程证明了：设 $p\nmid h(-D)$，这里 $h(-D)$ 表示虚二次域 $\mathbf{Q}(\sqrt{-D})$ 的类数，则方程的整数解满足 $2|x$. 由此可以得到(A) 中取减号的方程在 $p>2,2<D<100$ 时的全部整数解（此时仅有解 $p=5,D=31,x=2,y=\pm 1$）. 对于 $p=3$ 的情形，柯召和孙琦、曹珍富与刘培杰均证明了：设 $D>0$ 不被 $6k+1$ 形素数整除，则(A)除 $x^3+1=y^2$ 仅有正整数解 $(x,y)=(2,3)$ 和 $x^3+1=2y^2$ 仅有正整数解 $(x,y)=(1,1),(23,78)$ 外，其他均无正整数解. 在此之前，Nagell 与 Ljunggren 只解决了部分特殊例子. 当 D 含有 $6k+1$ 形的素因子时，方程

(B) $$x^3\pm 1=Dy^2,xy\neq 0$$

的求解将变得困难. 例如 Ljunggren 用了复杂且不初等的方法才证明方程 $x^3-1=7y^2$ 仅有正整数解 $(x,y)=(2,1),(4,3),(22,39)$. 这个结果能否有初等且简洁的证明？当 $D=31$ 时，(B) 中取加号的方程易 证无整数解（参见任冬的文献），而(B) 中取减号的方程却非常困难. 1983 年，J. A. Antoniadis 在研究类数2的虚二次

域中，提出如下猜想：方程 $x^3-1=31y^2$ 仅有整数解 $(x,y)=(1,0)$，$(5,2)$，$(5,-2)$（见 *J. Reine Angew. Math.*，339(1983)，27-81；*MR* 85g：11098）. 1988年，de Weger 用 Baker 方法证明这个猜想是正确的. 但 de Weger 的证明十分复杂，能否给出初等的证明或较为简洁的证明①？一般地，当 p 是 $6k+1$ 形的素数且 $3\mid h(-p)$ 时，如何确定方程 $x^3-1=py^2$ 的全部整数解？在 $p<100$ 时，这样的素数仅有 31，61，那么如何确定方程 $x^3-1=61y^2$ 的全部整数解？Nagell 在 $3\nmid h(-p)$ 时，证明方程 $x^3-1=py^2$ 的全部整数解满足 $2\mid x$，所以在 $3\nmid h(-p)$ 时，如果 $p\equiv 7 \pmod 8$ 且是具有 $6k+1$ 形的素数，那么方程 $x^3-1=py^2$ 的全部整数解又如何确定？在 $p<100$ 时这样的素数仅有 7，31，79. 从解决 $p=7,31$ 的情况来看，解决 79 看来也是不容易的. 对于方程

$$x^3 \pm 8 = Dy^2 \tag{C}$$

当 $D>2$ 无平方因子且不被 $6k+1$ 形的素数整除时，柯召和孙琦在一些条件下证明了 (C) 仅有 $y=0$ 的整数解. 曹珍富给出了方程 (C) 在 $D=p$ 或 $3p$，$p=3$ 或 $p\equiv 5 \pmod 6$，p 是素数时的全部整数解，例如方程 $x^3-8=3y^2$ 仅有正整数解 $x=11$，$y=21$；方程 $x^3+8=Dy^2$ 除 $13^3+8=5\cdot 21^2$ 外无其他的正整数解，等等. 曹珍富在《丢番图方程引论》（217 页）中认为：利用递推序列的方法可以给出 $D>0$ 且不被 $6k+1$ 形的素数整除时方程 (C) 的全部整数解. 因此他猜想：设 $D>0$ 且 D 不被 $6k+1$ 形的素数整除，则最多只有有限个这样的 D 使方程 (C) 有正整数解.

[1] 曹珍富 (Z. Cao)，丢番图方程引论，哈尔滨工业大学出版社，1989；*MR*92e：11018.

[2] 曹珍富 (Z. Cao)，数论中的若干新的问题和结果，河池师专学报，1987，1：1-8.

① 此问题已于最近被曹珍富与牟善志解决.

[3]曹珍富(Z. Cao),On the Diophantine equation $x^{2n}-Dy^2=1$, *Proc. Amer. Math. Soc.*, 98(1986), 1:11-16; *MR* 87i:11035.

[4]曹珍富(Z. Cao),丢番图方程与实二次域类数的可除性,数学学报,37(1994),5:625—631.

[5]曹珍富(Z. Cao),王笃正,关于丢番图方程 $x^{2n}-Dy^2=1$ 和 $x^2-Dy^{2n}=1$,扬州师院自然科学学报,1985,2:16—18; *MR* 89f:11048.

[6]曹珍富(Z. Cao),关于丢番图方程 $x^p-y^p=Dz^2$,东北数学,2(1986),2:219 — 227; *MR* 88b:11013.

[7]曹珍富(Z. Cao),Ljunggren 方程及其推广,哈尔滨电工学院学报,11(1988),2:184—189; РЖ Мат. 1989, 4A 103.

[8]曹珍富(Z. Cao),刘培杰(P. Liu),一个 Diophantus 方程的初等解法,山东师大学报(自然科学版),4(1989),1:13—16.

[9]曹珍富(Z. Cao),关于方程 $7x^2+1=y^p, xy\neq 0$,西南师范学院学报(自然科学版),1985,2:70—73.

[10]曹珍富(Z. Cao),关于方程 $Dx^2\pm 1=y^p, xy\neq 0$,数学研究与评论,7(1987),3:414.

[11]柯召(Chao Ko),孙琦(Q. Sun),关于丢番图方程 $x^3\pm 1=Dy^2$,中国科学,1981,12:1453—1457.

[12]柯召(Chao Ko),孙琦(Q. Sun),关于丢番图方程 $x^3\pm 1=3Dy^2$,四川大学学报(自然科学版),1981,2:1—5.

[13]柯召(Chao Ko),孙琦(Q. Sun),关于丢番图方程 $x^3\pm 8=Dy^2$ 和 $x^3\pm 8=3Dy^2$,四川大学学报(自然科学版),1981,4:1—5.

[14]乐茂华(M. Le), A note on the diophantine equation $x^{2p}-Dy^2=1$, *Proc. Amer. Math. Soc.*, 107(1989), 1:27-34.

[15]W. Ljunggren, Sätze über unbestimmte Gleichungen, *Skr. Norske Vid. Akad. Oslo. I.* 1942, 9:55pp.

[16]T. Nagell, Über die rationaler punkte auf einigen kubischen kurven, *Tohoku Math. J.*, 24(1924), 48-53.

[17] T. Nagell, Sur I' impossibilite de quelques équations à deux indéterminécs, *Norsk mat. forenings skrifter*, serie I, 1921(13).

[18]任冬(D. Ren),关于方程 $x^3\pm 1=Dy^2$(Ⅱ),朝阳师专学报,1990,3:57-60.

[19]孙琦(Q. Sun),关于方程 $15x^2+1=y^p$ 和 $23x^2+1=y^p$,四川大学学报(自然科学版),1987,1:19－23.
[20]B. M. M. de Weger, A Diophantine equation of Antoniadis, *Number Theory and application*(Banff,AB,1988),575-589. *NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci.*, 265, Kluwer Acad. Publ., Dordrecht, 1989; *MR* 92f: 11048.

D26. 商高数组猜想

我国古代《周髀算经》就提出了商高定理"勾三股四而弦五",这给出了方程 $x^2+y^2=z^2$ 的一组正整数解 $x=3,y=4,z=5$. 一般地,将满足 $x^2+y^2=z^2$ 的数组 (x,y,z) 称为商高数组. 1956年, Sierpinski 首先证明了 $3^x+4^y=5^z$ 仅有正整数解 $x=y=z=2$. Jesmanowicz 证明了对于 $(a,b,c)=(5,12,13),(7,24,25),(9,40,41),(11,60,61)$,方程

$$a^x+b^y=c^z \tag{A}$$

均仅有正整数解 $x=y=z=2$. 注意到这里的 (a,b,c) 是特殊类型的商高数组 $(2n+1,2n(n+1),2n(n+1)+1)$ 当 $1\leqslant n\leqslant 5$ 时的情形, Jesmanowicz 对一般的商高数组 (a,b,c),提出了如下猜想:方程(A) 均仅有正整数解 $x=y=z=2$.

对于商高数组

$$a=2n+1,b=2n(n+1),c=2n(n+1)+1,n>0, \tag{B}$$

柯召(1958)证明了:在 $n\equiv 1,3,4,5,7,9,10,11 \pmod{12}$,或 $n\equiv 2 \pmod 5, 3 \pmod 7, 4 \pmod 9, 5 \pmod{11}, 6 \pmod{13}, 7 \pmod{15}$ 时,商高数组猜想成立. 由此可推出 $n<96$时猜想成立. 饶德铭利用柯召的方法证明了在 $n\equiv 2,6 \pmod{12}$ 时猜想也成立. 1964年,柯召、孙琦讨论了 (B) 中数剩下的情形,证明了 $n<1000$时猜想成立. 稍后,柯召又把1000改进为6144. 1965年, Dem'janenko 证明了对 (B) 中的商高数组猜想成立,他还同时证明了对于

$$a=m^2-1,b=2m,c=m^2+1,m>1, \tag{C}$$

猜想成立. 在此之前,陆文端解决了 $m=2n$ 的情形,而 Jozefiak 比陆文端晚两年只解决了 (C) 中数组的特殊情形: $m=2^r p^s$, r,s 是正整数, p 是素数. 柯召(1959)首先考虑了更为一般的商高数组

(D) $a=s^2-t^2, b=2st, c=s^2+t^2, s>t>0, (s,t)=1, 2\nmid s+t$ 证明了:设 $s=2n$ 和 t 均不含 $4k+1$ 形素因子,且

1) $n\equiv 2 \pmod 4$, $t\equiv 3 \pmod 8$,或

2) $n\equiv 2 \pmod 4$, $t\equiv 5 \pmod 8$, $2n+t$ 含 $4k-1$ 形素因子,或

3) $n\equiv 0 \pmod 4$, $t\equiv 3,5 \pmod 8$,

则猜想成立. 对于 $s=3n, t=2m$, 他也得出类似的结论. 陈景润、曹珍富等用柯召的方法讨论了若干新的情形.

Nobuhiro Terai 提出了另一个猜想为:设 a,b,c 是两两互素的商高数组, $2|a$, 则方程

$$x^2+b^m=c^n \tag{E}$$

仅有正整数解 $(x,m,n)=(a,2,2)$, 并且对于 $b^2+1=2c, b<20, c<200$ 证明了这个猜想是正确的;当 b 和 c 均是素数且满足 $b^2+1=2c$, 及 $d=1$ 或当 $b\equiv 1 \pmod 4$ 时 d 为偶数,则猜想也是正确的,这里 d 是 $\mathbf{Q}(\sqrt{-b})$ 的理想类群中 $[c]$ 的一个素因子的阶. 1995 年末曹珍富与董晓蕾证明了:当 b,c 中有一个为素数或素数幂,且 $c\equiv 5 \pmod 8$ 时 Terai 猜想成立. 当 c 是素数时,对于任意的正整数 b, 孙琦与曹珍富曾给出了方程(E) 的较为一般的解答;乐茂华证明了:如果 $\max(b,c)>\exp\exp\exp 1000$, 那么

1) 当 $b=3u^2+1, c=4u^2+1, u$ 是正整数时,方程(E) 最多有三组正整数解

$(m,n,x)=(1,1,u), (1,3,8u^2+3u), (m_3,n_3,x_3)$, 这里 $2|m_3$;

2) 当 $b=2, c=2^{2^r}+1, r$ 是正整数时,方程(E) 恰有两组正整数解 $(m,n,x)=(2^r,1,1), (2^r+2,2,2^{2^r}-1)$;

3) 除1), 2)外, (E) 最多有两组正整数解 (m_1,n_1,x_1) 与 (m_2,n_2,x_2), 且 $m_1\not\equiv m_2 \pmod 2$.

但是，一般地证明 Jesmanowicz 与 Terai 关于商高数组的这两个猜想是非常困难的.

戴宗恕与曹珍富提出了另一个猜想：如果正整数 a,b,c,x,y,z 满足 $a^2+2b^2=c^2$，$a^x+2b^y=c^z$ 和 $a\neq 1$，那么 $x=y=z=2$. 显然 $a=2n^2+4n+1$，$b=2n(2n+1)$，$c=6n^2+4n+1$，$n>0$ 适合 $a^2+2b^2=c^2$ 且 $a\neq 1$，他们证明：在 $n\not\equiv 0 \pmod 4$ 时，所提猜想是正确的. 他们也考虑更一般猜想的提法：设正整数 a,b,c,x,y,z 适合 $a^2+Db^2=c^2$，$a^x+Db^y=c^z$ 和 $a\neq 1$，这里 D 是任意的正整数，则 $x=y=z=2$.

[1]曹珍富(Z. Cao)，丢番图方程引论，第九章 § 2，§ 4，哈尔滨工业大学出版社，1989; *MR* 92e:11018.

[2]曹珍富(Z. Cao)，关于商高数猜想的一个结论，数学通讯，1982，6:35—36.

[3]曹珍富(Z. Cao)，董晓蕾(X. Dong)，On Terai's conjecture，to appear.

[4]陈景润(J. Chen)，关于 Jesmanowicz 猜想，四川大学学报(自然科学版)，1962，2:19—25.

[5]戴宗恕(Z. Dai)，曹珍富(Z. Cao)，关于丢番图方程 $(2n^2+4n+1)^x+2(2n(2n+1))^y=(6n^2+4n+1)^z$，哈尔滨工业大学学报，1982，4:96—101.

[6]V. A. Dem'janenko，On Jesmanowicz' problem for Pythagorean numbers (Russian)，*Izv. Vyss Ucebn. Zaved. Matematika*，48(1965)，5:52-56.

[7]L. Jesmanowicz，Kilda uwag o liczbach pitagorejskich [Some remarks on Pythagorean numbers]，*Roczn. Polsk. towarz. mat*. [Wiakom. Mat.]，1(1956)，Ser. 2，2:196-202.

[8]T. Jozefiak，On a hypothesis of L. Jesmanowicz concerning Pythagorean numbers，*Prace Mat.*，5(1961)，119-123.

[9]柯召(Chao Ko)，关于商高数，四川大学学报(自然科学版)，1958，1:73—80

[10]柯召(Chao Ko)，关于 Jesmanowicz 的猜测，四川大学学报(自然科学版)，1958，2:31—40.

[11]柯召(Chao Ko)，关于商高数 $2n+1, 2n(n+1), 2n(n+1)+1$，四川大

学学报(自然科学版),1963,2:9 — 13;高等学校自然科学学报,数学、力学、天文版,1(1965),4:346 — 349.
[12]柯召(Chao Ko),孙琦(Q.Sun),关于商高数 $2n+1,2n(n+1),2n(n+1)+1$(Ⅱ),四川大学学报(自然科学版),1964,3:1 — 6.
[13]柯召(Chao Ko),关于商高数 $2n+1,2n(n+1),2n(n+1)+1$(Ⅲ),四川大学学报(自然科学版),1964,4:11 — 24.
[14]柯召(Chao Ko),关于丢番都方程 $(a^2-b^2)^x+(2ab)^y=(a^2+b^2)^z$,四川大学学报(自然科学版),1959,3:25 — 34.
[15]乐茂华(M.Le),The diophantine equation $x^2+D^m=p^n$, *Acta Arith.*, 52(1989),3:255-265.
[16]陆文端(W.Lu),论商高数 $4n^2-1,4n,4n^2+1$,四川大学学报(自然科学版),1959,2:39—42.
[17]饶德铭(D.Rao),关于丢番都方程 $(2n+1)^x+(2n(n+1))^y=(2n(n+1)+1)^z$ 的一点注记,四川大学学报(自然科学版),1960,1:79—80.
[18]W.Sierpinski,O rownaniu $3^x+4^y=5^z$ [On the equation $3^x+4^y=5^z$], *Roczn. Polsk. towarz. mat.* [Wiadom. Mat.],1 (1956), Ser. 2, 2: 194-195.
[19]孙琦(Q.Sun),曹珍富(Z.Cao),关于方程 $x^2+D^m=p^n$ 和 $x^2+2^m=y^n$,四川大学学报(自然科学版),1988,2:164 — 169; *MR* 89j:11029.
[20]Nobuhiro Terai, The diophantine equation $x^2+q^m=p^n$, *Acta Arith.*, 63(1993),4:351-358.

D27. 方程 $n=x^2+y^2-z^2,x^2\leqslant n,y^2\leqslant n,z^2\leqslant n$

由于 $(k+1)^2-k^2=2k+1,1+k^2-(k-1)^2=2k$,故把正整数 n 表成 $n=x^2+y^2-z^2$ 的形状是永远可能的,这里 x,y,z 都是整数. P. Erdös 给柯召写信提出下面的问题:是否对充分大的正整数 n,都有整数 x,y,z 存在,使得

$$(A)\qquad n=x^2+y^2-z^2,x^2\leqslant n,y^2\leqslant n,z^2\leqslant n?$$

柯召从具体计算中发现,在 $n\leqslant 10000$ 时有“76”个数不能表成(A)的形状,这里“76”加了引号,原因是:我们发现,柯召的“76”个数中有两个数(189 与 223)有误,因为

$$189=9^2+12^2-6^2,223=6^2+14^2-3^2,$$

而这两个数应分别为187与222. 其次，佟瑞洲用计算机检验发现，在 $n < 10^5$ 时有下列 77 个数不能表成(A)的形状：

3,6,11,15,22,27,35,38,42,55,59,66,78,83,87,95,110,118,123,131,143,150,187,210,222,227,255,262,266,278,299,303,323,326,395,402,447,483,502,551,563,590,618,635,678,735,755, 838,843,867,902,930,942,1003, 1007, 1034, 1091,1162,1190,1295,1326,1482,1523,1770,1790,2067,2103,2407,2483,2598,2782,3422,3495,4686,5447,5727,6563

即柯召得到的表中漏了150，且将187与222分别误为189与223. 除了上述的计算，柯召还进行了以下讨论：设

$$a^2 \leqslant n = a^2 + b < (a+1)^2,$$

则在 $b = 4m$ 与 $b = 2m + 1$ 时分别有

$$n = a^2 + (m+1)^2 - (m-1)^2, n = a^2 + (m+1)^2 - m^2,$$

且容易验证 (A) 中的其他条件；而在 $b = 4m + 2$ 时，设 $2a + 4m + 1 = kl, 1 \leqslant k \leqslant l$，则有

$$n = (a-1)^2 + \left(\frac{l+k}{2}\right)^2 - \left(\frac{l-k}{2}\right)^2.$$

当 $a \geqslant 4, k \geqslant 3$ 时易知 $\left(\frac{l+k}{2}\right)^2 \leqslant n$，故在 $a \geqslant 4$ 时只有当

(B) $n = a^2 + 4m + 2, 1 \leqslant 2m + 1 \leqslant a$ 且 $2a + 4m + 1$ 为素数

时才有可能不适合(A). 由此易知，设 $A(N)$ 为小于 N 且不能表为 (A) 的形状的正整数 n 的个数，则 $A(N) = O\left(\frac{N}{\ln N}\right)$. 柯召对于适合(B)的 n，讨论了表成(A)的充要条件，由此提出了如下的猜想："充分大的正整数 n 均能表成(A)的形状. 6563很可能是不能表为(A)的最大整数". 证明或否定这个猜想是很难的，即使对于 $a^2 + 2$，要证明充分大的 a，$a^2 + 2$ 均能表为(A)的形状亦很难.

[1]曹珍富(Z. Cao)，丢番图方程引论，哈尔滨工业大学出版社，1989，182—185；MR 92e:11018.

[2]柯召(Chao Ko),关于方程$n=x^2+y^2-z^2,x^2\leqslant n,y^2\leqslant n,z^2\leqslant n$,四川大学学报(自然科学版),1959,6:1-10.

D28. 相关学科中的某些丢番图方程问题

(1)整树中的问题. 设G是图,$P(G,x)$是图G的特征多项式,如果$P(G,x)=0$的所有解都是整数,则图G称为整图. Capobianco 等人在《公开问题的一个收集》(*A collection of open problems*, Annals of New York Academy of Science, 1980)一书的第582—583页中,列出的第23个问题是:直径3的树$T(m,r)$是由一条新边联结两个星图$K_{1,m}$和$K_{1,r}$的中心得到图. 当$m<r$时,有人使用计算机很费力地找到了$T(m,r)$为整树的65组解(m,r). 直径4的树$S(r,m)$是联结r个星图$K_{1,m}$的中心到一个新顶点得到的图,当且仅当m和$m+r$都是平方数时$S(r,m)$是直径4的整树. 存在直径大于4的整树吗?存在异于$S(r,m)$的直径4的整树吗?当$m<r$时能否给出全部直径3的整树$T(m,r)$?李学良与林国宁给出了一棵异于$S(r,m)$的直径4的整树,同时给出了一类直径6的整树,这就部分地回答了上述问题. 他们提出了另外两个问题:存在直径5的整树吗?存在直径为任意大的整树吗?曹珍富给出丢番图方程组

$$(A)\qquad \begin{cases}a^2+b^2=m+r+1,\\ a^2b^2=mr,m<r,a<b,\end{cases}$$

的全部正整数解为

$$(B)\qquad m=d\left(\frac{y_k-y_l}{2}\right)^2,r=d\left(\frac{y_k+y_l}{2}\right)^2,$$

$$a=\frac{x_k-x_l}{2},b=\frac{x_k+x_l}{2},$$

这里$k>l>0$是整数,$y_k\equiv y_l\pmod 2$,x_n与y_n由下式定义

$$x_n+y_n\sqrt{d}=\varepsilon^n,n=1,2,\cdots,$$

$\varepsilon=x_0+y_0\sqrt{d}$为 Pell 方程$x^2-dy^2=1$的基本解. 从而给出全部直径3的整树$T(m,r)$. 稍后,刘儒英利用(A)的特殊解,即(B)中$d=2,k=l+1$时的情形,给出了一类直径5的整树. 曹珍富利用

解(B)得出了迄今最为广泛的直径5的整树和一类新的直径6的整树.为了回答是否有另外的直径5的整树的问题,他考虑了由一条新边联结两个直径4的树$S(r,m)$和$S(k,l)$的中心得到的直径5的树,证明了此时不存在直径5的整树.

设$S(m_1,\cdots,m_r)$是联结r个星图$K_{1,m_1},\cdots,K_{1,m_r}$的中心到一个新顶点的直径4的树.曹珍富给出$m_1=a(a+1)-\eta,r=a(a+1)+\eta,m_2=\cdots=m_r=1,\eta\in\{-1,1\}$时$S(m_1,\cdots,m_r)$是直径4的整树.能否给出$S(m_1,\cdots,m_r)$的更为一般的结果?当$m_2=m_3=\cdots=m_r$时,$S(m_1,\cdots,m_r)$为整树的充要条件是:$m_2$是一个完全平方数且$x^4-(m_1+m_2+r)x^2+m_1(r-1)+m_2(m_1+1)$能分解成$(x^2-a^2)(x^2-b^2)$.由此即知,需要求解丢番图方程组

$$(C)\qquad \begin{cases} a^2+b^2=m_1+m_2+r, \\ a^2b^2=m_1(r-1)+m_2(m_1+1), \end{cases}$$

这里m_2为完全平方数.能否给出(C)的全部正整数解?这是一个很难回答的问题,即使在$m_2=1$时,即(C)成为

$$(D)\qquad \begin{cases} a^2+b^2=m_1+r+1 \\ a^2b^2=m_1r+1, b>a. \end{cases}$$

要给出(D)的全部正整数解也不容易((D)显然有无穷多组正整数解$m_1=a(a+1)\pm1,r=a(a+1)\mp1,b=a+1$).

(2)**差集中的问题**.1962年,Whiteman在不同特征的两个有限域的直和$GF(p^a)\oplus GF(p^b)$中引进了广义分圆(cyclotomy).Whiteman考虑的是Z中的特殊情形$e=(p-1,q-1)$,因而建立了一类循环(cyclic)的差集.1967年,Storer在他的书《分圆与差集》(*Cyclotomy and Difference sets*, Markham, Chicago, 1967)中,推广了Whiteman差集,建立了如下的定理:设p^a和$q^b=3p^a+2$是素数幂,那么在$GF(p^a)\oplus GF(q^b)$中存在一个参数为

$$v=p^aq^b, k=\frac{v-1}{4}, \lambda=\frac{v-5}{16}$$

的差集,其中k是一个奇数平方.这种差集称为Storer差集.1992年,

Jungnickel 指出：至目前为止，Storer 差集均是 Whiteman 差集且仅知道的例子分别是 $p=17, q=53$；和 $p=46817, q=140453$. Storer 证明当 $p^a < 341804080817$ 时没有别的例子. 曹珍富证明了 Storer 差集均是循环情形，即均是 Whiteman 差集，证明中主要使用他关于丢番图方程的一些成果. 例如他证明了联立方程组

$$(E)\qquad \begin{cases} q^b = 3p^a + 2 \\ p^a q^b - 1 = 4x^2, 2 \nmid x \end{cases}$$

蕴涵 $a=b=1$，其中 p, q 是素数，a, b 是正整数. 他同时考虑 Whiteman 差集在更大范围内的个数，证明了：当 $p < 2U_{22}^2 - 1$（此数大于 1.8×10^{25}）时仅当 $(p,q) = (17,53), (46817,140453)$，和 $(2U_{13}^2 - 1, 6U_{13}^2 - 1)$ 时 Whiteman 差集存在，这里 U_n 满足 $U_0 = 1, U_1 = 3, U_{n+2} = 4U_{n+1} - U_n$. 但是 Whiteman 差集是有限个还是无限个，却是不易回答的问题.

在 Jungnickel 关于差集的长篇综述中，列为猜想13.9的是两个数论猜想，即：设 p 是奇素数，$a \geqslant 0, b, t, r \geqslant 1$，那么

(a) $Y = 2^{2a+2}p^{2t} - 2^{2a+2}p^{t+r} + 1$ 是一个平方数当且仅当 $t=r$；

(b) $Z = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1$ 是一个平方数当且仅当 $p=5$，$b=3, t=1, r=2$（即 $Z=2401$）.

这是马少麟在对可逆差集当 $v \neq 4n (n = k - \lambda)$ 时的公开问题的研究中提出来的，并且证明：如果 (a) 与 (b) 均正确，那么可逆差集当 $v \neq 4n$ 时仅有参数(4000,775,150). 曹珍富证明了猜想 (a) 与 (b)，因而解决了可逆差集当 $v \neq 4n$ 时的公开问题.

但是，我们不知道一般的丢番图方程

$$(F)\qquad x^2 = p_1^{\alpha_1} \cdots p_s^{\alpha_s} - p_1^{\beta_1} \cdots p_s^{\beta_s} + 1, p_i (i = 1, \cdots, s) \text{ 是不同素数}$$

如何求解？这里 $\alpha_i, \beta_i (i = 1, \cdots, s)$ 均是正整数，x 是整数.

(3)利用有限单群的分类定理，对于给定形式阶的单群的刻划是一个重要课题. 段学复教授早就指出，确定哪些单群的阶不恰含素数的一次幂是一个非常困难的问题. 陈重穆证明了：有限单群 G 的阶均不为 $k(k \geqslant 3)$ 次幂，且 G 的阶为平方数的充分必要条件是

G 为 Lie 型单群 $B_2(p)$，p 为适合丢番图方程 $p^2-2r^2=-1$ 的素数. 那么方程 $p^2-2r^2=-1$ 当 p 为素数时有多少解？有限多还是无限多？回答这个问题很难，甚至回答 p,r 均为素数的解是有限的还是无限的也很困难. 1986 年，屈明华证明了：当 $p,r<10^{15}$ 时仅有三对素数解 $(p,r)=(7,5)$，$(41,29)$ 和 $(63018038201, 44560482149)$. 曹珍富还提出了一个类似的问题，即是否存在无穷多对素数 p,r 适合 $p^2-5r^2=-4$？

对于确定给定形式阶的单群，也需要求解若干类的丢番图方程. 设 $p_1,\cdots,p_t$ 是给定的素数，确定阶 $\prod_{i=1}^{t}p_i^{\alpha_i}$ 与 $(\prod_{i=1}^{t}p_i^{\alpha_i})p^{\alpha}$ 的单群，这里 $\alpha_i(i=1,\cdots,t)$ 与 α 均为正整数，p 是素数且 $p\notin\{p_1,\cdots,p_t\}$，依赖于求解如下的丢番图方程：

$$(G)\qquad S_1-S_2=2, S_1,S_2\in S^*,$$

这里

$$S^*=\{x\mid x=p_1^{x_1}\cdots p_t^{x_t}, x_i\in Z_{\geqslant 0}(i=1,\cdots,t)\}.$$

曹珍富利用他自己关于方程 $ax^2-by^2=2$ 的结果，其中 $a\neq 2$，且 $x\mid^* a$，或 $y\mid^* b$，符号 $x\mid^* a$ 表示 x 的每一个素因子整除 a，给出了上述方程的一般的求解算法. 设 (G) 的解集为 $S(p_1,\cdots,p_t)$，利用已经求出的 $S(p_1,\cdots,p_t)$，他还给出确定阶为 $(\prod_{i=1}^{t}p_i^{\alpha_i})p^a r^b$ 的单群算法，这里 $p,r\notin\{p_1,\cdots,p_t\}$ 是任意的两个素数. 当 $(\prod_{i=1}^{t}p_i^{\alpha_i})$ 最多有一个 $4k+1$ 形、最多有一个 $6k+1$ 形的素因子时，除 Lie 型单群 $A_1(q)$ 外，其余均可有统一算法确定. 而 $A_1(q)$ 的确定依赖于下列丢番图方程的求解：

$$(H)\qquad q(q^2-1)=(2,q-1)(\prod_{i=1}^{t}p_i^{\alpha_i})p^a r^b,$$

$$a,b,\alpha_i(i=1,\cdots,t)\in Z_{>0},$$

这里 q 是素数幂，$(2,q-1)$ 表 2 与 $q-1$ 的最大公约数. 给出方程 (H) 全部解是较为困难的. 特别地，当 $t=2, p_1=2, p_2=3$ 时方程

(H) 解的个数是有限还是无限?这也是一个不易回答的问题.

[1]曹珍富(Z. Cao),关于直径 $R(3 \leqslant R \leqslant 6)$ 的整树,黑龙江大学学报(自然科学版),1988,2:1—3,95; *MR* 90e:11039.

[2]曹珍富(Z. Cao),直径为5,6的整树的一些新类,系统科学与数学,11(1991),1:20—26; *MR* 92f:05035.

[3]曹珍富(Z. Cao),差集中的一些不定方程问题,全国第五届组合数学学术会议论文摘要汇编,上海同济大学,1994年5月30日—6月4日.

[4]曹珍富(Z. Cao),关于阶为 $2^{a_1}3^{a_2}5^{a_3}7^{a_4}p^{a_5}$ 的单群,数学年刊,A 辑,16(1995),2:244—250.

[5]曹珍富(Z. Cao),关于方程 $ax^m - by^n = 2$,科学通报,35(1990),7:558—559; *Chinese Sci. Bull.*,35(1990),14:1227 — 1228; *Zbl.* 764. 11020.

[6]曹珍富(Z. Cao),邓谋杰,关于数组 $(n+1, n-1)$ 问题的机器解法,在曹珍富主编的《中国科协首届青年学术年会卫星会议暨哈尔滨第二届青年学术年会论文集(理工分册)》中,哈尔滨工业大学出版社,1992,1 — 6.

[7]M. Capobianco, S. Maurer, D. McCarthy and J. Molluzzo, *A collection of open problems*, Annals of New York Academy of Science, 1980, 582-583.

[8]陈重穆(C. Chen),关于有限单群的阶,数学学报,30(1987),5:605—613.

[9]D. Jungnickel, Difference Sets, In J. H. Dinitz and D. R. Stinson(eds.), *Contemporary Design Theory: A collection of Surveys*, John Wiley & Sons, Inc. 1992, 241-324.

[10]李学良(X. Li),林国宁,关于整树问题,科学通报,1987,11:813—316.

[11]刘儒英(R. Liu),直径为5的整树,系统科学与数学,1988,4:357—360.

[12]S. L. Ma, McFarland's Conjecture on abelian difference sets with multiplier —1, *Designs, Codes and Crypt.*, 1(1992), 321—332.

[13]屈明华(M. Qu),关于丢番图方程 $p^2 - 2q^2 = -1$,四川大学学报(自然科学版),1986,2:1—9.

[14]施武杰(W. Shi),关于单 K_4 —群,科学通报,36(1991),17:1281—1283.

[15]J. Storer, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967.

[16]A. L. Whiteman, A family of difference sets, *Illinois J. Math.*, 6(1962), 107-121.

E 整数序列

这里，我们主要讨论无穷序列. 其中有些地方也许与 A 章和 C 章重叠了. 关于这方面曾有一本优秀的讲义，它是 H. Halberstam 和 K. F. Roth 著的《序列》第一卷（牛津大学出版社，1966）. 人们期待第二卷不久将会出版. 其他的参考文献是：

[1]P. Erdős, A. Sarközi and E. Szemerédi, On divisibility properties of sequences of integers, in Number Theory, *Colloq. Math. Soc. Janos Bolyai* 2, North-Holland, 1970, 35-49.

[2]H. Ostmann, *Additive Zahlentheorie* I, II, Springer-Verlag, Heidelberg, 1956.

[3]A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, I, II, *J. reine angew. Math.* 194(1955), 40-65, 111-140.

[4]Paul Turan (ed.) *Number Theory and Analysis; a collection of papers in honor of Edmund Landau* (1877-1938), Plenum Press, New York, 1969, contains several papers, by Erdős and others, on sequences of integers.

本节我们用 $A=\{a_i\}, i=1,2,\cdots$ 表一可能是无穷的严格递增非负整数序列. 不超过 x 的 a_i 的个数用 $A(x)$ 表示，而如果序列的密率存在，我们将用 $\lim A(x)/x$ 表示.

E1. $A(x)$的最大值

（1）如果序列每对元素的最小公倍数$[a_i,a_j]$至多为 x，那么 $A(x)$ 的最大值是多少？现已知

$$(9x/8)^{1/2} \leqslant \max A(x) \leqslant (4x)^{1/2}.$$

(2)假设序列$\{a_i\}$中,没有一个元素能除尽其他 r 个元素的乘积,则 Erdös 证明了

$$\pi(x)+c_1x^{2/(r+1)}(\ln x)^{-2}<\max A(x)<\pi(x)+c_2x^{2/(r+1)}(\ln x)^{-2}$$

其中,$\pi(x)$ 是$\leqslant x$ 的素数个数. 可是,如果我们假定,不大于 r 的任意个 a_i 的乘积是不同的,那么,$\max A(x)$ 为何? 对于 $r\geqslant 3$,Erdös 证明了:

$$\max A(x)<\pi(x)+O(x^{2/3+\epsilon}).$$

(3)Erdös 为下面问题的解决提供 50 美元奖金. 是否存在一足够稀的序列使 $A(x)<c\ln x$,而它的每一充分大的整数都可表成 $p+a_i$ 的形式,其中 p 是素数?

用 r 次幂来代替素数的类似问题已为 Leo Moser 解决,Ruzsa 已解决2的幂问题.

[1]P. Erdös, On sequences of integers no one of which divides the product of two others and on some related problems, *Inst. Math. Mec. Tomsk*, 2 (1938), 74-82

[2]P. Erdös, Problem, *Mat. Lapok*, 2(1951), 233.

[3]P. Erdös, Extremal problems in number theory V(Hungarian), *Mat. Lapok*, 17(1966), 135-155.

[4]P. Erdös, On some applications of graph theory, *to number theory*, *Publ. Ramanujan Inst.*, 1(11969), 131-136.

[5]L. Moser, On the additive completion of sets of integers, *Proc. Symp. Pure Math.*, 8 Amer. Math. Soc. Providence, 1965, 175-180.

[6]I. Ruzsa, On a problem of P. Erdös, *Canad. Math. Bull.*, 15(1972), 309-310

E2. 每个元素有两个可比因子的的序列

下列整数6,12,15,18,20,24,28,30,35,36,40,42,45,48,54,56,60,63,66,70,72,…

都有两个因子 d_1,d_2,使得 $d_1<d_2<2d_1$. 它们的密率为1吗?Er-

dős 已证明其密率存在. 该问题与覆盖同余有关(F12).

[1]P. Erdős, On the density of some sequences of integers, *Bull. Amer. Math. Soc.*, 54(1948), 685—692; *MR* 10, 105.

E3. 与给定序列有关的序列

假设 $D(x)$ 是不大于 x，且可被至少一个 a_i 除尽的那些数的个数，其中 $a_1 < a_2 < \cdots < a_k \leqslant n$ 是给定的序列，那么 $D(x)/x < 2D(n)/n$ 对全部 $x > n$ 成立吗?2不能被去掉，例如 $n = 2a_1 - 1$，$x = 2a_1 < a_2$. 另一方面，已知对每一 $\varepsilon > 0$，存在一个序列，它不满足不等式 $D(x)/x > \varepsilon D(n)/n$ (参阅[1]、[2]).

设 $n_1 < n_2 < \cdots$ 是一整数序列，它使得当 $i \to \infty$ 时，$n_{i+1}/n_i \to 1$，且 $\{n_i\}$ 对每一个 d 是不均匀分布的(mod d). [$n_i \leqslant x$，且 $n_i \equiv c$ (mod d)的 n_i 的个数 $N(c,d;x)$ 满足:

$$N(c,d;x)/N(1,1;x) \to 1/d (x \to \infty \text{ 时})$$

对每个 c 和所有 d 成立，其中 $0 \leqslant c \leqslant d-1$]. 如果 $a_1 < a_2 < \cdots$ 是满足 $a_j + a_k \neq n_i$ (对于任意的 i,j,k)的无穷整数序列，那么 Erdős 问，a_j 的密率小于1/2吗?

[1]A. S. Besicovitch, On the density of certain sequences, *Math. Ann.*, 110(1934), 355-341

[2]P. Erdős, Note on sequences of integers no one of which is divisible by any other, *J. London Math. Soc.*, 10(1935), 126-128.

E4. 一个与素数有关的级数与序列

如果 p_n 表第 n 个素数，Erdős 问 $\sum(-1)^n n/p_n$ 是否收敛?

他又问，给定三个不同素数，如果将它们幂的积按递增排列为 $a_1 < a_2 < a_3 < \cdots$，那么 a_i 与 a_{i+1} 都是素数幂的情形会出现无穷多次吗?如果我们用 k 个素数或甚至无穷多个素数来代替三个素数

又会如何呢?Meyer 和 Tijdeman 对于两有限素数集合 S 和 T 问了类似的问题,此时 $a_1 < a_2 < \cdots$ 是取自 $S \cup T$,存在无穷多个 i,使得 a_i 是来自 S 中的素数幂的乘积,而 a_{i+1} 却是 T 中的素数幂的积吗?

E5. 和不为平方数序列

Paul Erdös 和 David Silverman 考虑 k 个整数 $1 \leqslant a_1 < a_2 < \cdots < a_k \leqslant n$ 使得 $a_i + a_j$ 都不是平方数的问题,并问:$k < n(1+\varepsilon)/3$ 或甚至 $k < n/3 + O(1)$ 为真吗?模 3 为 1 的整数表明,如果它为真,那么,它便是可能达到的最好结果. 他们认为,对于不是平方数的其他序列可以问同样的问题.

Erdös 和 Graham 在他们的书中说,J. P. Marsias 已发现,任何两个 $\equiv 1,5,9,13,14,17,21,25,26,29,30 \pmod{32}$ 整数的和决不是一个平方数(mod32),因此,k 至少可选作 $11n/32$. 因为 J. Lagarias, A. M. Odlyzko 和 J. Shearer 已证明,如果 $S \subseteq Z_n$ 且 $S+S$ 不含 Z_n 的平方数,那么 $|S| \leqslant 11n/32$,所以 Marsias 的结果是能达到的最好结果.

E6. Roth 猜想

K. F. Roth 猜想,必存在绝对常数 c 使得对每一个 k,存在 $n_o = n_o(k)$ 具有下面的性质:对于 $n > n_o$,分解不超过 n 的整数成 k 类 $\{a_i^{(j)}\}(1 \leqslant j \leqslant k)$,那么对某些 j,可写成形如 $a_{i_1}^{(j)} + a_{i_2}^{(j)}$ 的不超过 n 的不同整数的个数必大于 cn.

E7. 含算术级数的序列

由著名的 van der Waerden 定理知,对每个 l,存在 $n(h,l)$ 使得,如果不超过 $n(h,l)$ 的整数被分成 h 类,那么至少有一类包含有 $l+1$ 项的算术级数(AP). 更一般地,给定 $l_0, l_1, \cdots, l_{h-1}$,总存在类 $V_i (0 \leqslant i \leqslant h-1)$,它含有一个有 $l_i + 1$ 项的 AP. 用 $W(h,l)$,

或更一般地，用 $W(h;l_0,l_1,\cdots,l_{h-1})$ 表最小的这样的 $n(h,l)$.

Chvátal 计算出 $W(2;2,2)=9$, $W(2;2,3)=18$, $W(2;2,4)=22$, $W(2;2,5)=32$ 和 $W(2;2,6)=46$. Beeler 和 O'Neil 给出，$W(2;2,7)=58$, $W(2;2,8)=77$ 和 $W(2;2,9)=97$. $W(2;3,3)=35$ 和 $W(2;3,4)=55$ 也是 Chvátal 找到的. $W(2;3,5)=73$是 Beeler 和 O'Neil 算出的，Stevens 和 Shentaram 找到了，$W(2;4,4)=178$，Chvátal 找到 $W(3;2,2,2)=27$，Brown 找到 $W(3;2,2,3)=51$. Beeler 和 O'Neil 又找到 $W(4;2,2,2,2)=76$.

van der Waerden 的定理的许多证明仅给出了 $W(h,l)$ 的粗略估计，Erdös 和 Rado 证明了 $W(h,l)>(2lh^l)^{1/2}$，而 Moser, Schmidt 和 Berlekamp 将界逐渐改进到

$$W(h,l)>lh^{c\ln h} \text{ 和 } W(h,l)>h^{l+1-c\sqrt{(l+1)\ln(l+1)}}.$$

Moser 的界（$l\geqslant 5$）已由 Abbott 和 Liu 改进到

$$W(h,l)>h^{c_s(\ln h)^s},$$

其中 s 由 $2^s\leqslant l<2^{s+1}$ 定义. Everts 已证明，$W(h,l)>lh^l/4(l+1)^2$. 该结果有时比 Berlekamp 的结果要好.

一个与此紧密联系的函数（$l+1=k$）便是著名的 $r_k(n)$，它是 Erdös 和 Turán 很多年前引入的，它表示不超过 n 的 r 个数$1\leqslant a_1<a_2<\cdots<a_r\leqslant n$ 构成的序列必含有 k 项 AP 的最小的 r. 当 $k=3$时，最好的界是 Behrend, Roth 和 Moser 找到的，即

$$n\exp(-c_1\sqrt{\ln n})<r_3(n)<c_2n/\ln\ln n,$$

且对于大的 k，Rankin 证明了

$$r_k(n)>n^{1-c_s/(\ln n)^{s/(s+1)}},$$

其中 s 由 $2^s<k\leqslant 2^{s+1}$ 定义.

此问题的重大突破是 Szemerédi 获得的. 他证明了，对全部 k，$r_k(n)=o(n)$. 但是，无论是 Szemerédi, Furstenberg，还是 Katznelson 和 Ornstein（看 Thouvenot 的文章）的证明，都没有给出 $r_k(n)$ 的估计量. Erdös 猜想：对每一个 t，

$$r_k(n) = o(n(\ln n)^{-t}).$$

这将推出，对每一个 k，在 AP 中存在 k 个素数（见 A5中 Erdös 的有奖猜想，如果该猜想为真，则可推出 Szemerédi 定理）.

另一个与此关系比较密切的问题是 Leo Moser 研究的，他把整数写成以3为基的形式：$n = \sum a_i 3^i (a_i = 0, 1$，或$2)$，并且考虑将 n 映射成无穷维 Euclid 空间的格点$(a_1, a_2, a_3, \cdots)$. 如果一些映象是共线的，则他称对应的那些整数为共线的. 如，35→(2,2,0,1,0,…)，41→(2,1,1,1,0,…)和47→(2,0,2,1,0,…)是共线的. 他猜想，不具有3个共线数的整数序列的密率为0. 如果一些整数是共线的，则它们在 AP 中. 但是逆命题不一定成立. 如：16→(1,2,1,0,0…)，24→(0,2,2,0,0,…)和32→(2,1,0,1,0,…)不是共线的. 因此，此猜想如为真，则推出 Roth 定理：$r_3(n) = o(n)$.

如果 $f_3(n)$ 是每边有三个点的 n 维立方体中无三点在一条线上的格点的最大个数，那么 Moser 证明了 $f_3(n) > c3^n/\sqrt{n}$，容易看出，$f_3(n)/3^n$ 趋于某一有限值，那么，它趋于零吗？Chvátal 改进 Moser 结果中的常数 c 为$3/\sqrt{\pi}$. 并且找到了 $f_3(1)=2$，$f_3(2)=6$，$f_3(3)=16$. 现还知道 $f_3(4) \geqslant 43$.

更一般地，如果 n 维立方体在每边上有 k 个点，Moser 问 $f_k(n)$ 的估计是多少？这里 $f_k(n)$ 表没有 k 个点共线的格点的最大个数. 由 Hales 和 Jewett 定理知，对充分大 n，将 k^n 个格点任意分成 h 类，则必有一类其 k 个点是共线的. 由此推出了 van der Waerden 关于格点$(a_0, a_1, \cdots, a_{n-1})(0 \leqslant a_i \leqslant k-1)$与以 k 为基的整数的展开式 $\sum a_i k^i$ 对应起来的定理.

如果用贪心算法去构造不含 AP 的序列，不能得到非常稠密的，但却能得到一些令人感兴趣的序列. Odlyzko 和 Stanley 构造正整数序列 $S(m)$：$a_0 = 0, a_1 = m$，且每一后继项 a_{n+1} 都是比 a_n 大的最小整数. 因此，$a_0, a_1, \cdots, a_{n+1}$ 不含有三项 AP，例如，

$S(1)$：0,1,3,4,9,10,12,13,27,28,30,31,36,39,40,81,82,

84,85,…

$S(4)$:0,4,5,7,11,12,16,23,26,31,33,37,38,44,49,56,73,78,80,85,…

如果 m 是3的幂,或是3的幂的2倍,那么序列的成员在它们三元展开的项中是非常易于描述的.但是,对于其他的值,序列则变得相当不稳定.其增长速率似乎是类似的,但这有待于证明.

不含有4项 AP 的"最简单"的序列是:

0,1,2,4,5,7,8,9,14,15,16,18,25,26,28,29,30,33,36,48,49,50,52,53,55,56,57,62,…

存在此序列的简单描述吗?它增长多快?

如果我们定义集合 S 的跨度为 $\max S - \min S$,那么不包含 k 项 AP 的 n 个整数的集合的最小跨度 $sp(k,n)$ 是多少?Zalman Usiskin 给出下列值

n	=	3	4	5	6	7	8	9	10	11 …
$sp(3,n)$	=	3	4	8	10	12	13	19	24	25 …
$sp(4,n)$	=		4	5	7	8	9	12 …		

$sp(k,n)$ 是函数 $r_k(n)$ 的反函数.

[1]H. L. Abbott and D. Hanson, Lower bounds of certain types of van der Waerden numbers, *J. Combin. Theory*, 12(1972),143-146.

[2]H. L. Abbott and A. C. Liu, On partitioning integers into progression free sets, *J. Combin. Theory*, 13 (1972),432-436.

[3]H. L. Abbott, A. C. Liu and J. Riddell, On sets of integers not containing arithmetic progressions of prescribed length, *J. Austral. Math. Soc.*, 18(1974),188-193; *MR* 57#12441.

[4]Michael D. Beeler and Patrick E. O' Neil, Some new van der Waerden numbers, *Discrete Math.*, 28(1979),135-146.

[5]F. A. Behrend, On sets of integers which contain no three terms in

arithmetical progression, *Proc. Nat. Acad. Sci. USA*, 32(1946), 331-332; *MR* 8, 317.

[6]E. R. Berlekamp, A construction for partitions which avoid long arithmetic pro-gressions, *Canad. Math. Bull.*, 11(1968), 409-414.

[7]E. R. Berlekamp, On sets of ternary vectors whose only linear dependencies involve an odd number of vectors, *Canad. Math. Bull.*, 13 (1970), 363-366.

[8]Thomas C. Brown, Some new Van der Waerden numbers, *Notices Amer. Math. Soc.*, 21(1974), A-432.

[9]T. C. Brown, Behrend's theorem for sequences containing no k-element progression of a certain type, *J. Combin. Theory*, Ser. A, 18(1975), 352-356.

[10]Ashok K. Chandra, On the solution of Moser's problem in four dimensions, *Canad. Math. Bull.*, 16(1973), 507-511.

[11] V. Chvátal, Some unknown van der Waerden numbers, in *Combinatorial Structures and their Applications*, Gordon and Breach, New York, 1970, 31-33

[12]V. Chvátal, Remarks on a problem of Moser, *Canad. Math. Bull.*, 15 (1972), 19-21.

[13]J. A. Davis, Roger C. Entringer, Ronald L. Graham and G. J. Simmons, On permutations containing no long arithmetic progressions, *Acta Arith.*, 34(1977/78), 81-90; *MR* 58#10705.

[14]P. Erdős, Some recent advances and current problems in number theory, in *Lectures on Modern Mathematics*, Wiley, New York, 3(1965), 196-244.

[15]P. Erdős and R. Rado, Combinatorial theorems on classifications of subsets of a given set, *Proc. London Math. Soc.* (3)2(1952), 417-439; *MR*16, 445.

[16]P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, 1974, 37-39.

[17]P. Erdős and P. Turán, On some sequences of integers, *J. London Math. Soc.*, 11(1936), 261-264.

[18]F. Everts, PhD thesis, University of Colorado, 1977.

[19]H. Furstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. Analyse Math.*, 31(1977), 204-256; *MR* 58#16583.

[20]Joseph L. Gerver and Thomas L. Ramsey, Sets of integers with nonlong arithmetic progressions generated by the greedy algorithm, *Math. Comp.*, 33(1979), 1353-1359; *MR* 80k:10053.

[21]R. L. Graham and B. L. Rothschild, A survey of finite Ramsey Theorems, *Congressus Numerantium III*, Proc. 2nd Louisiana Conf. Combin., Graph Theory, Comput, (1971), 21-40.

[22]R. L. Graham and B. L Rothschild, A short proof of van der Waerden's theorem on arithmetic progressions, *Proc. Amer. Math. Soc.*, 42(1974), 385-386.

[23]G. Hajós, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Z.*, 47(1942), 427-467.

[24]A. W. Hales and R. I. Jewett, Regularity and positional games, *Trans. Amer. Math. Soc.*, 106(1963), 222-229.

[25]A. Y. Khinchin, *Three Pearls of Number Theory*, Graylock Press, Rochester, N. Y., 1952, 11-17.

[26]L. Moser, On non averaging sets of integers, *Canad. J. Math.*, 5 (1953), 245-252.

[27]Leo Moser, Notes on number theory Ⅱ. On a theorem of van der Waerden, *Canad. Math. Bull.*, 3(1960), 23-25; *MR* 22#5619.

[28]L. Moser, Problem 21, Proc. Number Theory Conf. Univ. of Colorado, Boulder, 1963, 79

[29]L. Moser, Problem 170, *Canad. Math. Bull.*, 13(1970), 268.

[30]A. M. Odlyzko and R. P. Stanley, Some curious sequences constructed with the greedy algorithm, Bell. Labs. internal memo., 1978

[31]Carl Pomerance, Collinear subsets of lattice point sequences—an analog of Szemerédi's theorem, *J. Combin. Theory Ser. A*, 25(1980), 140-149.

[32]John R. Rabung, On applications of van der Waerden's theorem, *Math. Mag.*, 48(1975), 142-148.

[33]John R. Rabung, Some progression-free partitions constructed using Folkman's method, *Canad. Math. Bull.*, 22(1979), 87-91.

[34]R. Rado, Note on combinatorial analysis, *Proc. London Math. Soc.*, 48(1945), 122-160.

[35]R. A. Rankin, Sets of integers containing not more than a given number of terms in arithmetical progression, *Proc. Roy. Soc. Edinburgh Sect. A*, 65(1960/61), 322-334; *MR*26 # 95.

[36]J. Riddell, On sets of numbers containing nolterms in arithmetic progressions, *Nieuw Arch. Wisk.* (3)17(1969), 204-209; *MR*41 # 1678.

[37]R. F. Roth, Sur quelques ensembles d'entiers, *C. R. Acad. Sci. Paris*, 234(1952), 388-390.

[38]R. F. Roth, On certain sets of integers, *J. London Math. Soc.*, 28 (1953), 104-109; *MR*14, 536(and see *ibid*, 29(1954), 20-26; *J. Number Theory*, 2(1970), 125-142; *Period. Math. Hungar*, 2(1972), 301-326).

[39]R. Salem and D. C. Spencer, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. USA*, 28(1942), 561-563; *MR*4, 131.

[40]R. Salem and D. C. Spencer, On sets which do not contain a given number in arithmetical progression, *Nieuw Arch. Wisk.* (2)23(1950), 133-143.

[41]H. Salie, Zur Verteilung natürlicher Zahlen auf Elementfremde Klassen, *Ber. Verh. Sächs. Akad. Wiss. Leipzig*, 4 (1954), 2-26.

[42]Wolfgang M. Schmidt, Two combinatorial theorems on arithmetic progressions, *Duke Math. J.*, 29 (1962), 129-140

[43]G. J. Simmons and H. L. Abbott, How many 3-term arithmetic progressions can there be if there are no longer ones? *Amer. Math. Monthly*, 84 (1977), 633-635; *MR* 57 # 3056.

[44]R. S. Stevens and R. Shantaram, Computer generated van der Waerden partitions, *Math. Comp.*, 32(1978), 635-636.

[45]E. Szemeredi, On sets of integers containing no four terms in arithmetic progression, *Acta Math. Acad. Sci. Hungar*, 20(1969), 89-104.

[46]E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.*, 27(1975), 199-245.

[47]J. P. Thouvenot, La démonstration de Furstenberg du théorème de Szemerédi sur les progressions arithmétiques, *Springer Lect. Notes in Math.*, 710, Berlin, 1979, 221-232; *MR* 81c:10072.

[48]B. L. van der Waerden, Beweis einer Baudet'schen Vermutung, *Nieuw Arch. voor Wisk.* II 15(1927), 212−216.

[49]B. L. van der Waerden, How the proof of Baudet's conjecture was found, in *Studies in Pure Mathematics*, Academic Press, London, 1971, 251-260.

[50]E. Witt, Ein kombinatorische Satz der Elementargeometrie, *Math. Nachr.*, 6(1952), 261-262.

E8. Schur 问题、整数无和类

Schur 证明了，如果小于 $n!e$ 的整数以任意方式分成 n 类，那么 $x+y=z$ 必能在某一类内得到整数解. 如果 $s(n)$ 是具有此类性质的最小整数，Abbott 和 Moser 证明了对某些 c 和充分大的 n，$s(n)>89^{n/4-c\ln n}$，Abbott 和 Hanson 证明了 $s(n)>c(89)^{n/4}$，这一结果改进了 Schur 自己的估计 $s(n)\geqslant(3^n+1)/2$. Schur 的结果事实上对 $n=1,2,3$ 它是强的，但对较大的 n，则不行了. $s(4)=45$ 是 Baumert 计算出来的. 例如，头44个数可被拆成4个无和类：

{1,3,5,15,17,19,26,28,40,42,44}, {2,7,8,18,21,24,27,33,37,38,43}, {4,6,13,20,22,23,25,30,32,39,41}, {9,10,11,12,14,16,29,31,34,35,36}.

最近，Fredericksen 证明了 $s(5)\geqslant158$(见 E9)，并且对所有的后继 Schur 数，该结果改进了下界：

$$s(n)\geqslant c(315)^{n/5}(n>5).$$

Robert Irving 稍稍改进了 Schur 的上界 $[n!e]$ 为 $[n!(e-1/24)]$.

[1]H. L. Abbott, phD thesis, University of Alberta, 1965.

[2]H. L. Abbott and D. Hanson, A problem of Schur and its generalizations, *Acta Arith.*, 20(1972), 175-187.

[3]H. L. Abbott and L. Moser, Sum-free sets of integers, *Acta Arith.*, 11 (1966), 393-396; *MR* 34# 69.

[4]L. D. Baumert, Sum-free sets, *J. P. L. Res. Summary No* 36-10, 1 (1961), 16-18.

[5]S. L. G. Choi, The largest sum-free subsequence from a sequence of n numbers, *Proc. Amer. Math. Soc.*, 39(1973), 42-44; *MR* 47# 1771.

[6]S. L. G. Choi, J. Komlós and E. Szemerédi, On sum-free subsequences, *Trans. Amer. Math. Soc.*, 212(1975), 307-313.

[7]H. Fredericksen, Five sum-free sets, *Proc. 6th Ann. S.E. Conf. Graph Theory, Combin. & Comput. Congressus Numerantiun XIV*, Utilitas Math. Pub. Inc 1975, 309-314.

[8]R. W. Irving, An extension of Schur's theorem on sum-free partitions, *Acta Arith.*, 25(1973), 55-63.

[9]J. Komlós, M. Sulyod and E. Szemerédi, Linear problems in combinatorial number theory, *Acta Math. Acad. Sci. Hungar*, 26(1975), 113-121.

[10]L. Mirsky, The combinatorics of arbitrary partitions, *Bull. Inst. Math. Appl.*, 11(1975), 6-9..

[11]I. Schur, Über die Kongruenz $x^m + y^m \equiv z^m \pmod p$. *Jahresb. der Deutsche Math.-Verein.* 25(1916), 114-117.

[12]W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room Squares, Sun-free Sets, Hadamard Matrices*, Springer-Verlag, Heidelberg, 1972.

[13]Š. Znám, Generalisation of a number-theoretic result, *Mat.-Fyz. Časopis*, 16(1966), 357-361.

[14]Š. Znám, On k-thin sets and n-extensive graphs, *Math. Časopis*, 17 (1967), 297-307.

E9. 整数模的无和类

Abbott 和 Wang 考虑了与 Schur 类似的问题. 设 $t(n)$ 是这样

的最小整数 m，它使得不管怎样把从1到 m 的整数分成 n 类，总存在一类包含有同余式

$$x + y \equiv z(\mathrm{mod}(m+1))$$

的解. 显然 $t(n) \leqslant s(n)$，这里 $s(n)$ 的定义同 E8，但对 $n=1,2$ 或 3，我们有 $t(1)=s(1)=2, t(2)=s(2)=5, t(3)=s(3)=14$. 确实，仅存在[1,13]的三种分为三个集合的方式

$$\{1,4,10,13\},\{2,3,11,12\},\{5,6,8,9\}$$

（这里7分别在三个集中）满足无和条件. 且它们满足更严格的无同余条件(mod14). 而 Baumert 的例子(E8)仅在第二个集合中有一个反例：$33+33 \equiv 21(\mathrm{mod}45)$. 实际上 Baumert 找到了112种分解[1,44]成4个无和集合的方式，其中一些对模45无和. 因此，$t(4)=45$，一个例子是

$\{\pm1,\pm3,\pm5,15,\pm17,\pm19\},\{\pm2,\pm7,\pm8,\pm18,\pm21\},\{\pm4,\pm6,\pm13,\pm20,\pm22,30\},\{\pm9,\pm10,\pm11,\pm12,\pm14,\pm16\}$.

Abbott 和 Wang 得到不等式

$$f(n_1+n_2) \geqslant 2f(n_1)f(n_2)$$

对 $f(n)=s(n)-1/2$ 成立，且对 $t(n)$ 能导出与 Schur 对 $s(n)$ 导出的相同的下界：$t(n) \geqslant (3^n+1)/2$. 实际上，他们已得到 $t(n)=s(n)$ 的例子. 此外，Fredericksen 有如下的例子：

$\pm\{1,4,10,16,21,23,28,34,40,43,45,48,54,60\},\pm\{2,3,8,9,14,19,20,24,25,30,31,37,42,47,52,65,70\},\pm\{5,11,12,13,15,29,32,33,35,36,39,53,55,56,57,59,77,79\},\pm\{6,7,17,18,22,26,27,38,41,46,50,51,75\},\pm\{44,49,58,61,62,63,64,67,68,69,71,72,73,74,76,78\}$.

这表明 $s(5) \geqslant 158$，且模 159 是无和的. 因而 $t(5) \geqslant 158$ 和 $t(n) > c(315)^{n/5}$.

[1]H. L. Abbott and E. T. H. Wang, Sum-free sets of integers, *Proc. Amer. Math. Soc.*, 67(1977), 11-16; *MR* 58#5571.

E10. 强无和类

Turán 已证明，如果整数 $[m, 5m+3]$ 以任意方式分为两类，那么，至少在一类中，方程

$$x + y = z$$

有 $x \neq y$ 的解. 且这对于 $[m, 5m+2]$ 不真. $[m, 5m+2]$ 分解成两无和集合的唯一性已被 Znám 证实.

Turán 又研究了 x, y 不一定是不相同的问题. 定义 $s(m,n)$ 为这样的最小整数，它使得无论 $[m, m+s]$ 被怎样的分为 n 类，这 n 类中必有一类包含 $x+y=z$ 的一个解. 他的与头一个问题对应的结果是 $s(m,2)=4m$. 显然，$s(1,n)=s(n)-1$，其中 $s(n)$ 的定义仍见 E8. 由 Irving 的结果推出 $s(m,n) \leqslant m[n!(e-1/24)-1]$. Abbott 和 Znám(见 E8)分别找到 $s(m,n) \geqslant 3s(m,n-1)+m$，从而 $s(m,n) \geqslant m(3^n-1)/2$.

如果某类不含有方程 $x+y=z$ 或 $x+y+1=z$ 的解，则 Abbott 和 Hanson 称其为强无和的. 他们证明了，如果 $r(n)$ 是这样的最小的 r，它使得无论 $[1,r]$ 怎样分成 n 类，他们中必有一类含有上述方程的解，则 $r(m+n) \geqslant 2r(n)s(m)-r(n)-s(m)+1$. 他们用此改进了 $s(m,n)$ 的下界. 他们的方法结合 Fredericksen 的例子给出 $s(m,n) > cm(315)^{n/5}$.

[1] Š. Znám, Megjegyzések Turán Pál egy publikálatlan ereményéhez, *Mat. Lapok*, 14(1963), 307-310.

E11. van der Waerden 和 Schur 问题的推广

Rado 研究了 van der Waerden 和 Schur 问题的若干推广. 例如，他证明了，对任意自然数 a, b, c，必存在 u，使得无论 $[1, u]$ 怎

---

① 此不等式在 Richard K. Guy 的书(E13)中误为 $s(m,n) \geqslant 3s(m,n)+m$.

样分成两类都有，至少在一类中 $ax+by=cz$ 有解. 他给出了 u 的一个值，但象 Schur 的问题一样，这还不是可能达到的最好的结果. 例如，对于 $2x+y=5z$，从定理有 $u=20$，而它对于 $u=15$ 也为真，尽管对更小的 u 它不成立：下列二集合

$$\{1,4,5,6,9,11,14\} \text{ 和 } \{2,3,7,8,10,12,13\}$$

中没有一个包含 $2x+y=5z$ 的解. 如果我们允许分成三类，那么 45 便是这样的最小的 u 值：

{1,4,5,6,9,11,14,16,19,20,21,24,26,29,31,34,36,39,41,44},

{2,3,7,8,10,12,13,15,17,18,22,23,27,28,32,33,37,38,42,43},

{6,7,8,9,25,30,35,40}.

对于方程 $\sum a_i x_i = 0$，其中 a_i 是非零整数，如果存在一个 $u(n)$（我们假定它为最小的）使得区间 $[1,u(n)]$ 无论怎样分成 n 类，都至少有一类包含方程的解，则 Rado 称此方程为 n- 正则的. 又如果方程对所有的 n 都是 n- 正则的，那么称方程是正则的，并且他证明了，恰好当 $\sum a_j = 0$ 对某些 a_i 的子集成立时，方程是正则的. 例如，对 $a_1=a_2=1$ 且 $a_3=-1$，我们对 Schur 的原问题有 $u(n)=s(n)$. Salié 和 Abbott 研究了找 $u(n)$ 下界的问题，见 E7和 E8所附文献.

上面例子当 $a_1=2, a_2=1, a_3=-5$ 时不是正则的. 因为我们可以看出，它是2-正则和3-正则的，但不是4-正则的. 如把 $5^k l$ 的每一个数（其中 $5 \nmid l$）按照 k 是奇或偶和 $l \equiv \pm 1$ 或 $\pm 2 \pmod 5$ 分成四类，可以证明，这四类中没有一类含有 $2x+y=5z$ 的解.

对于方程 $2x_1+x_2=2x_3$ 和 $x_1+x_2+x_3=2x_4$，Salié, Abbott 及 Abbott 和 Hanson 相继得到较好的下界，最后分别得到 $u(n) > c(12)^{n/3}$ 和 $c(10)^{n/3}$.

可将问题 E7—12与 C13—15比较.

[1]Walter Deuber, Partitionen und lineare Gleichungssysteme, *Math. Z.*, 133(1973), 109-123.

[2]R. Rado, Studien zur Kombinatorik, *Math. Z.*, 36(1933), 424-480.

[3]E. R. Williams, M. Sc. thesis, Memorial Univ., 1967.

E12. Lenstra 序列

Lenstra 注意到,递推关系 $x_0 = 1, x_n = (1 + x_0^2 + x_1^2 + \cdots + x_{n-1}^2)/n(n = 1,2,\cdots)$[或$(n+1)x_{n+1} = x_n(x_n + n)$]产生 $x_1 = 2$, $x_2 = 3, x_3 = 5, x_4 = 10, x_5 = 28, x_6 = 154, x_7 = 3520, x_8 = 1551880, x_9 = 267593772160, \cdots$ 且 x_n 对于 $n \leqslant 42$ 都为整数,但 x_{43} 却不是整数. Alf van der Poorten 问,若继续下去,情形会如何呢? Davfd Boyd 问:是否 x_n 总是2-adic 整数(即它的分母不含有2).

Boyd 和 van der Poorten 研究了用立方代替平方后的对应序列.

E13. Collatz 序列

L. Collatz 问,由 $a_{n+1} = a_n/2(a_n$ 为偶$), a_{n+1} = 3a_n + 1(a_n$ 为奇) 定义的序列,如果就从任意整数 a_1 起,必存在一个 n 使 $a_n = 1$ 的意义上来看,序列除开圈4,2,1,4(图10,见下页)外,是否为树状结构?D. H. Lehmer 和 Emma Lehmer 和 J. L. Selfridge 证实了这对所有小于10^9的整数为真.另一些人将界推至7×10^{11}.设最小的正整数 k 使 $a_k = 1$(如果存在的话),则 k 称为 a 的长度,记为 $l(a)$,这里 $a = a_1$.当 k 不存在时,记 $l(a) = \infty$. Filipponi 用十分简单的方法研究长度相同的一些数以及小的可能的 a_0 使 $l(a_0) = \infty$.例如从 Filipponi 结果知

$$l(64k+15) = l(192k+45),$$
$$l(256k+98) = l(256k+99)$$
$$= l(256k+100) = l(256k+101),$$
$$l(4^n3^{-n}(4^{3^{n-1}k} - 1) + 1) = 2(n + k3^{n-1}),$$

图10. Collatz 序列是树状吗?

且　　$a_0 = 4k+3, k \not\equiv 0 \pmod 4$ 和 $k \not\equiv 0 \pmod 8$.

Filipponi 提出如下的猜想:存在正常数 c 使得

$$a^{-1}\sum_{i=1}^{a} l(i) \sim c \ln a.$$

如果用$3a_n - 1$ 替代 $3a_n + 1$(或我们包括非负整数),那么任何序列以下面其中一个圈为终止似乎是可能的:{1,2},{5,14,7,20,10},或{17,50,25,74,37,110,55,164,82,41,122,61,182,91,272,236,68,34}. 这对所有比10^8小的数已证明为真.

David Kay 更一般地用 $a_{n+1} = a_n/p(p \mid a_n), a_{n+1} = a_n q +$

$r(p\nmid a_n)$ 定义了序列，并问是否存在数 p,q,r 使该问题能获解决？

定义 $f(n)$ 为 $3n+1$ 的最大奇因子，Zimian 问，是否 $\prod_{i=1}^{m} n_i = \prod_{i=1}^{m} f(n_i)$ 对于整数 $n_i>1$ 的任意一个（或多个）集 $\{n_i\}$ 成立. Erdös 找到

$65\times7\times7\times11\times11\times17\times17\times13=49\times11\times11\times17\times17\times13\times13\times5$.

如果对某些 $k\geqslant1$，有 n 除尽 $f^k(n)$，则称 n 为自包含的. 如果出现了这样的整数，且 Collatz 序列 $n^* = f^k(n)/n$ 达到1，那么集合

$$\{n,f(n),\cdots,f^{k-1}(n),n^*,f(n^*),\cdots,1\}$$

便是上述那样的集合. 用计算机已经找到了$\leqslant10^4$的5个自包含的整数31，83，293，347和671.

[1]Michael Beeler, William Gosper and Rich Schroeppel, Hakmem, Memo 239, Artificial Intelligence Laboratory, M. I. T., 1972, p. 64.

[2]Corrado Böhm and Giovanna Sontacchi, On the existence of cycles of given length in integer sequences like $x_{n+1}=x_n/2$ if x_n even, and $x_{n+1}=3x_n+1$ otherwise, *Atti Accad. Naz. Lincei Rend. Sci. Fis. Mat. Natur.* (8)64(1978), 260-264.

[3]R. E. Crandall, On the "$3x+1$" problem, *Math. Comp.*, 32(1978), 1281-1292; *MR* 58#494; *Zbl*. 395. 10013.

[4]C. J. Everett, Iteration of the number-theoretic function $f(2n)=n$, $f(2n+1)=3n+2$, *Advances in Math.* 25(1977), 42-45; *MR* 56#15552; *Zbl*. 352. 10001.

[5]P. Filipponi, On the $3n+1$ problem: something old, something new, *Rend. Mat. Appl.* (7)11(1991), 1:85—103.

[6]Martin Gardner, Mathematical Games, A miscellany of transcendental problems. simple to state but not at all easy to solve, *Scientific Amer.*, 226#6(Jun 1972), 114-118, esp p. 115.

[7]E. Heppner, Eine Bemerkung zum Hasse-Syracuse-Algorithmus, *Arch. Math.* (Basel),31 (1977/79),317-320; *MR* 80d:10007; *Zbl.* 377.10027.
[8]David C. Kay, *Pi Mu Epsilon J.*, 5(1972), 338.
[9]J. C. Lagarias, *Amer. Math. Monthly*, 92(1985),1:3—23.
[10]H. Möller, Über Hasses Verallgemeinerung der Syracuse—Algorithmus (Kakutani's Problem), *Acta Arith.*, 34(1978),219—226; *MR*57# 16246; *Zbl.* 329. 10008.
[11]Ray P. Steiner, A theorem on the Syracuse problem, *Congressus Numerantium XX*, Proc. 7th Conf. Numerical Math. Comput. Manitoba, 1977,553-559; *MR* 80g: 10003.
[12]Riho Terras, A stopping time problem on the positive integers, *Acta Arith.*, 30(1976), 241-252; *MR* 58#27879 (and see 35(1979),100-102; *MR* 80h:10066).

E14. Conway 排列序列

在 Conway 的排列序列的情形里,情况与上一问题不同.一个简单的例子是 $a_{n+1}=3a_n/2$(a_n 为偶)且 $a_{n+1}=[(3a_n+1)/4]$(a_n 为奇),或也许更清楚地,

$$2m\to 3m,\quad 4m-1\to 3m-1,\quad 4m+1\to 3m+1.$$

从上明显看出,它的逆过程也成立.因此最终结构仅含有不相交圈和双无穷链.但是,仍不清楚是否存在有限或无限个上述的圈和链,或者,是否有无穷多个链存在.人们猜想,仅有的圈是{1},{2,3},{4,6,9,7,5}和{44,66,99,74,111,83,62,93,70,105,79,59}. Mike Guy 证明了,任何其他的圈其周期必大于320.下列含有8的序列又如何呢?

…,73,55,41,31,23,17,13,10,15,11,8,12,18,27,20,30,45,34,51,38,57,43,32,48,72,…

[1]J. H. Conway, Unpredictable iterations, in *Proc. Numer Theory Conf.*, Boulder, 1972, 49-52.

E15. Mahler 的 Z 数

Mahler 研究了下列问题：给定任意实数 α，设 r_n 是 $\alpha(3/2)^n$ 的小数部分，那么存在数 α 使得 $0 \leqslant r_n < 1/2$ 对所有 n 成立吗（这样的 α 如果存在，则称为 Z 数）？这个问题的回答一般倾向于否定. Mahler 证明了，在每对相邻整数中至多存在一个.

一个类似的问题是，存在有理数 r/s 使得 $[(r/s)^n]$ 对所有 n 是奇数吗？

Littlewood 问，e^n 的小数部分是否随 $n \to \infty$ 而趋于0？这个问题仍不清楚.

[1] K. Mahler, An unsolved problem on the powers of 3/2, *J. Austral. Math. Soc.*, 8(1968), 313-321; *MR* 37 # 2694.

E16. Whiteman 猜想

Forman 和 Shapiro 已证明，有无穷多个形如 $[(4/3)^n]$ 和 $[(3/2)^n]$ 的整数为合数，A. L. Whiteman 猜想，这两个序列都包含有无穷多个素数. 对于一般的 $a > b > 1$，a 和 b 为互素整数，$[(a/b)^n]$ 中是否有无穷多个合数？是否有无穷多个素数？

[1] W. Forman and H. N. Shapiro, An arithmetic property of certain rational powers, *Comm. Pure Appl. Math.*, 20(1967), 561-573; *MR* 35 # 2852.

E17. Davenport－Schinzel 序列

用 n 个字母 $[1, n]$ 来构成一 Davenport－Schinzel（D－S）序列，此序列中没有直接的重复 $\cdots aa \cdots$ 且没有长度大于 d 的交替序列 $\cdots a \cdots b \cdots a \cdots b \cdots$. 现用 $N_d(n)$ 表 D－S 序列的最大长度. 现在的问题是确定所有的 D－S 序列，特别是找到 $N_d(n)$ 为何.

序列12131323，12121213131313232323和 $1213141\cdots 1\,\overline{n-1}\,1\,\overline{n-1}\,\overline{n-2}\cdots 32n2n3n\cdots n\,\overline{n-1}\,n$ 表明 $N_4(3) \geqslant 8$，$N_8(3) \geqslant 20$ 和

$N_4(n) \geqslant 5n-8$. Davenport 和 Schinzel 证明了 $N_1(n)=1, N_2(n)=n, N_3(n)=2n-1, N_4(n)=O(n\ln n/\ln\ln n), \lim N_4(n)/n \geqslant 8$ 且和 J. H. Conway 证明了，$N_4(lm+1) \geqslant 6lm-m-5l+2$，因此 $N_4(n)=5n-8(4 \leqslant n \leqslant 10)$. Z. Kolba 证明了，$N_4(2m) \geqslant 11m-13$ 且 Mills 得到 $n \leqslant 21$ 时的 $N_4(n)$ 值. 例如序列

abacadaeafafedcbgbhbhgcicigdjdjgekekgfhijklkljlilhlfl

是 $N_4(12)=53$的证明的一部分.

Roselle 和 Stanton 固定 n 而不是 d，得到 $N_d(2)=d, N_d(3)=2[3d/2]-4(d>3), N_d(4)=2[3d/2]+3d-13(d>4)$ 且 $N_d(5)=4[3d/2]+4d-27(d>5)$. 可是，Peterkin 注意到最后一个括号内应是$(d>6)$，因为 $N_6(5)=34$. Roselle 和 Stanton 又证明了长为 $N_{2d+1}(5)$ 的序列是唯一的，而长为 $N_{2d+1}(4)$ 和 $N_{2d}(5)$ 的序列仅有两个.

Peterkin 列出了长为 $N_5(6)=29$ 的 56 个 D—S 序列，且证明了 $N_5(n) \geqslant 7n-13(n>5)$ 和 $N_6(n) \geqslant 13n-32(n>5)$.

Rennie 和 Dobson 给出了 $N_d(n)$ 的上界为：

$$(nd-3n-2d+7)N_d(n) \leqslant n(d-3)N_d(n-1) + 2n-d+2(d>3).$$

因此推广了 Roselle 和 Stanton 对 $d=4$时的结果.

除开已得到的特殊值，现在主要的问题是证明或否定 $N_d(n)=O(n)$，Szemerédi 证明了 $N_d(n)<c_d nL(n)$，其中 L 是最小的 e 的个数，它使 $e^{e^{\cdot^{\cdot^{e}}}}>n$.

表8　$N_d(n)$ 的值

d \ n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
3	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41

4	1 4 8 12 17 22 27 32 37 42 47 53 58 64 69 75 81 86 92 98 104
5	1 5 10 16 22 29
6	1 6 14 23 34
7	1 7 16 28
8	1 8 20 35
9	1 9 22 40
10	1 10 26 47

[1]H. Davenport, A combinatorial problem connected with differential equations II(ed. A. Schinzel), *Acta Arith.*, 17(1971),363-372.

[2]H. Davenport, and A. Schinzel, A combinatorial problem connected with differential equations, *Amer. J. Math.*, 87(1965),684-694.

[3]Annette J. Dobson and Shiela Oates Macdonald, Lower bounds for the lengths of Davenport-Schinzel sequences, *Utilitas Math.*, 6(1974),251-257.

[4] W. H. Mills, Some Davenport-Schinzel sequenees, *Congressus Numerantium IX*, Proc. 3rd Manitoba Conf. Numerical Math. 1973, 307-313; *MR* 50# 135.

[5] C. R. Peterkin, Some results on Davenport-Schinzel sequences, *Congressus Numerantium IX*, Proc. 3rd Manitoba Conf. Numerical Math. 1973, 337-344; *MR* 50# 136.

[6]B. C. Rennie and A. J. Dobson, Upper bounds for the lengths of Davenport-Schinzel sequences, *Utilitas Math.*, 8(1975),181-185.

[7]D. P. Roselle, An algorithmic approach to Davenport-Schinzel sequences, *Utilitas Math.*, 6(1974),91-93; *MR* 50# 9780.

[8]D. P. Roselle and R. G. Stanton, Results on Davenport-Schinzel sequences, *Congressus Numerantium I*, Proc. Louisiana Conf. Combin. Graph Theory, Comput. Baton Rouge, 1970, 249-267.

[9]R. G. Stanton and P. H. Dirksen, Davenport-Schinzel sequences, *Ars Combinatoria*, 1(1976),43-51.

[10]R. G. Stanton and R. C. Mullin, A map-theoretic approach to Davenport-Schinzel sequences, *Pacific J. Math.*, 40(1972), 167-172.

[11]R. G. Stanton and D. P. Roselle, A result on Davenport-Schinzel sequences. Colloq. Math. Soc. Janós Bolyai 4, *Combinatorial Theory and its Applications*, Balatonfüred, 1969, 1023-1027.

[12]R. G. Stanton and D. P. Roselle, Some properties of Davenport-Schinzel sequences, *Acta Arith.*, 17(1970-71), 355-362.

E18. Thue 序列

Thue 证明了存在无穷多个关于三个符号的序列,它不含有两个一致相等的相邻段.他又证明了存在无穷多个关于两个符号的序列它不含有三个一致相等的相邻段.其他许多人又重新发现这些结果.

如果不求一致相等段,而求不相邻段,其一段是另一段的排列,Justin 构造了一个关于两个符号的序列,它没有五个相邻段,其一段是另一段的排列.Pleasants 构造了关于5个符号的序列,它没有两个上述的相邻段.我们称 Justin 与 Pleasants 分别解决了(2,5)与(5,2)问题.

Dekking 已解决了(2,4)和(3,3)问题,但把(4,2)情形称之为"一个十分有趣的未决问题".存在关于4个符号序列,它不存在一个为另一个排列的相邻段吗?

[1]S. Arshon, Démonstration de l'éxistence des suites asymétriques infinies (Russian. French summary), *Mat. Sb.*, 2(44)(1937), 769-779.

[2]C. H. Braunholtz, Solution to problem 5030[1962, 439], *Amer. Math. Monthly*, 70(1963), 675-676.

[3]T. C. Brown, Is there a sequence on four symbols in which no two adjacent segments are permutations of one another? *Amer. Math. Monthly*, 78(1971), 886-888.

[4]Richard A. Dean, A sequence without repeats on x, x^{-1}, y, y^{-1}, *Amer.*

Math. Monthly, 72(1965),383-385.

[5]F. M. Dekking, On repetitions of blocks in binary sequences, *J. Combin. Theory Ser. A*, 20(1976),292-299.

[6]F. M. Dekking, Strongly non-repetitive sequences and progression-free sets, *J. Combin. Theory Ser. A*, 27(1979),181-185.

[7]R. C. Entringer, D. E Jackson and J. A. Schatz, On non-repetitive sequences, *J. Combin. Theory Ser. A*, 16(1974),159-164.

[8]P. Erdős, Some unsolved problems, *Magyar ud. Akad. Mat. Kutató Int. Közl.*, 6(1961),221-254,esp. p. 240.

[9]A. A. Evdokimov, Strongly asymmetric sequences generated by a finite number of symbols, *Dokl. Akad. Nauk SSSR*, 179(1968),1268-1271; *Soviet Math. Dok*1., 9(1968),536-539.

[10]Earl Dennet Fife, Binary sequences which contain no BBb, PhD thesis, Wesleyan Univ., Middletown, Connecticut, 1976.

[11]D. Hawkins and W. E. Mientka, On sequences which contain no repetitions, *Math. Student*, 24(1956),185-187;*MR* 19, 241.

[12]G. A. Hedlund, Remarks on the work of Axel Thue on sequences, *Nordisk Mat. Tidskr.*, 15(1967),147-150;*MR* 37#4454.

[13]G. A. Hedlund and W. H. Gottschalk, A characterization of the Morse minimal set, *Proc. Amer. Math. Soc.*, 16(1964),70-74.

[14]J. Justin, Généralisation du théoreme de van der Waerden sur les semi-groupes répétitifs, *J. Combin. Theory Ser A*, 12(1972),357-367.

[15]J. Justin, Semi-groupes répétitifs, *Sém. IRIA, Log. Automat.* 1971, 101-105,108; *Zbl.* 274.20092.

[16]J. Justin, Characterization of the repetitive commutative semigroups, *J. Algebra*, 21(1972) 87-90;*MR* 46#277; *Zbl.* 248.05004.

[17]John Leech, A problem on strings of beads, *Math. Gaz.*, 41(1957), 277-278.

[18]Marston Morse, A solution of the problem of infinite play in chess, *Bull. Amer. Math. Soc.*, 44(1938),632.

[19]Marston Morse and Gustav A. Hedlund, Unending chess, symbolic dynamics and a problem in semigroups, *Duke Math. J.*, 11(1944),1—7;

MR 5,202.

[20]P. A. B. Pleasants, Non-repetitive sequences, *Proc. Cambridge Philos. Soc.*, 68(1970), 267-274.

[21]Helmut Prodinger and Friedrich J. Urbanek, Infinite 0-1 sequences without long adjacent identical blocks, *Discrete Math.*, 28(1979), 277-289.

[22]H. E. Robbins, On a class of recurrent sequences, *Bull. Amer. Math. Soc.*, 43(1937), 413-417.

[23]A. Thue, Über unendliche Zeichenreihen, *Norse Vid. Selsk. Skr. I Mat.-Nat. Kl. Christiania* (1906), No. 7, 1-22.

[24]A. Thue, Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, Ibid, (1912), No. 1, 1—67.

E19. 算术级数覆盖整数

如果 S 是 n 个整数算术级数的并，每一个都有公差 $\geqslant k$，其中 $k \leqslant n$. Crittenden 和 Vanden Eynden 猜想，只要 S 含有 $\leqslant k \cdot 2^{n-k+1}$ 的那些整数，则 S 必含有所有正整数. 如果这为真，那么它是可能达到的最好结果. 他们已证明了 $k=1$ 的情形.

[1]R. B. Crittenden and C. L. Vanden Eynden, Any n arithmetie progressions covering the first 2^n integers covers all integers, *Proc. Amer. Math. Soc.*, 24(1970), 475-481.

[2]R. B. Crittenden and C. L. Vanden Eynden, The union of arithmetic progressions with differences not less than k, *Amer. Math. Monthly*, 79 (1972), 630.

E20. 无理序列

Erdös 和 Straus 定义，如果 $\sum 1/a_nb_n$ 对所有整数序列 $\{b_n\}$ 为无理数，则正整数序列 $\{a_n\}$ 为无理序列. 已找到一些有趣的无理序列. 如果 $\limsup(\log_2 \ln a_n)/n > 1$，那么 $\{a_n\}$ 为无理序列，其中 log 以2为底. $\{n!\}$ 不是无理序列，因为 $\sum 1/n!(n+2) = 1/2$.

Erdös 已证明 $\{2^{2^n}\}$ 是无理序列. 序列2,3,7,43,1807,…是无理序列吗?其中 $a_{n+1} = a_n^2 - a_n + 1$.

[1]P. Erdös, Some problems and results on the irrationality of the sum of infinite series, *J. Math. Sci.*, 10(1975), 1-7.

E21. Epstein 游戏

Richard Epstein 的"加或减一个平方数"的游戏是用一堆木片进行的. 两个人交替地从木片中加或减一个最大的完全平方数,也就是说,两人交替地命名非负整数 a_n, 其中 $a_{n+1} = a_n \pm [\sqrt{a_n}]^2$. 赢者是首先加或减到零的人. 这是一个循环游戏,许多数能导致平局,例如,从2开始,下一个人不能减1(那样对手便赢了),因此他加1而成3. 现在再加1又不行了,所以只有减1又回到2上去了. 类似地,6也会导致平局,最好的玩法是:6,10,19!,35,60,109!,209!,13!,22!,6,…(其中!表示一步最佳玩法而非阶乘). 例如,209后,405是不好的玩法,因为对手能够减至5,而5是前一个玩者必赢的位置(称为 $\mathscr{P}$-位置). 类似地,从60始,将数减至11也是不好的,因为11是后一个玩者必赢(走到20便可)的位置(称为 $\mathscr{N}$-位置).

$\mathscr{P}$-位置数

0,5,20,29,45,80,101,116,135,145,165,173,236,
257,397,404,445,477,540,565,580,585,629,666,
836,845,885,909,944,949,954,975,1125,1177,…

$\mathscr{N}$-位置数

1,4,9,11,14,16,21,25,30,36,41,44,49,52,54,64,69,71,81,84,86,92,100,105,120,121,126,136,141,144,149,164,169,174,189,196,201,208,216,225,230,245,252,254,256,261…
都有正密率吗?

[1]E. R. Berlekamp, J. H. Conway and Richard K. Guy, *Winning Ways*,

Academic Press, London, 1981, Chap. 15.

E22. B_2—序列

对于无穷序列$1 \leqslant a_1 < a_2 < \cdots$,如果 a_i 都不是序列中除开 a_i 的不同元素的和,那么称其为 A—序列. Erdős 证明了,对于每一个 A—序列,$\sum 1/a_i < 103$. Levine 和 O'Sullivan 改进此结果到$\sum 1/a_i < 4$. 他们又给出一个 A—序列,其倒数和>2.035,并且猜想,这几乎是对其极大值的正确回答.

如果$1 \leqslant a_1 < a_2 < \cdots$是 B_2—序列(参见 C8),即序列中所有 $a_i + a_j$ 是不同的,那么$\sum 1/a_i$ 的极大值是多少?视 $i = j$ 和 $i \neq j$ 而产生两类问题,Erdős 都不能解决.

最显而易见的 B_2—序列是由贪心算法得到的(见 E7;每一项都是比前一项大的最小整数,它不违背不同和条件,且允许 $i = j$)

1,2,4,8,13,21,31,45,66,81,97,123,148,182,…

Mian 和 Chowla 用此证明了存在 $a_k \ll k^3$ 的 B_2—序列. 如果 M 是$\sum 1/a_i$ 取遍 B_2—序列的极大值,且 S^* 是 Mian—Chowla 序列的倒数之和,那么 $M \geqslant S^* > 2.156$. 但是 Levine 注意到,如果 $t_n = n(n+1)/2$,那么 $M \leqslant \sum 1/(t_n + 1) < 2.374$,并希望看到人们对 $M = S^*$ 给出证明或反例.

[1]Eugene Levine, An extremal result for sum-free sequences, *J. Number Theory*, 12(1980),251-257.

[2]Eugene Levine and Joseph O'Sullivan, An upper estimate for the reciprocal sum of a sum-free sequence, *Acta Arith.*, 34(1977),9-24; *MR* 57 #5900; *Zbl.* 335. 10053.

[3]Abdul Majid Mian and S. D. Chowla, On the B_2 sequences of Sidon, *Proc. Nat. Acad. Sci. India Sect. A*, 14(1944), 3-4; *MR* 7-243.

[4]J. O'Sullivan, On reciprocal sums of sum-free sequences, PhD thesis,

Adelphi Univ. 1973.

E23. 和与积在同一类中的序列

如把整数分成两类，那么总存在序列$\{a_i\}$使得全部和$\sum \varepsilon_i a_i$与积$\prod a_i^{\varepsilon_i}$($\varepsilon_i = 0$或1)都是在同一类中吗？Hindman 否定地回答了 Erdös 的这一问题.

存在序列$a_1 < a_2 < \cdots$使得所有和$a_i + a_j$以及乘积$a_i a_j$都在同一类中吗？Graham 证明了，如果我们分整数[1,252]成两类，必存在4个不同的数$x, y, x+y$和xy是在同一类中. 此外，252是可能达到的最好的结果. Hindman 证明了，如果我们分整数[2,990]为两类，那么，其中一类总包含4个不同的数$x, y, x+y$和xy. 对于≥3的整数尚不知其相应的结果.

Hindman 又证明了，如果我们分整数成两类，那么总存在序列$\{a_i\}$使得所有的和$a_i + a_j$(允许$i = j$)在同一类中. 另一方面，他找到一种分成三类的分解法使得不存在上述的无穷序列.

[1] J. Baumgartner, A short proof of Hindman's theorem, *J. Combin Theory Ser. A*, 17(1974), 384-386.

[2] Neil Hindman, Finite sums with sequences within cells of a partition of *n*, *J. Combin. Theory Ser. A*, 17(1974), 1-11.

[3] Neil Hindman, Partitions and sums and products of integers, *Trans. Amer. Math. Soc.*, 247(1979), 227-245; *MR* 80b:10022.

[4] Neil Hindman, Partitions and sums and products—two counterexamples, *J. Combin. Theory Ser. A*, 29(1980), 113-120.

E24. MacMahon 序列

MacMahon 定义了如下序列：

1,2,4,5,8,10,14,15,16,21,22,25,26,28,33,34,35,36,38,40,42,…

它后继项中不包含前面所有两个或更多个相邻项的和.

如果 m_n 是此序列的第 n 个元素，且 M_n 是前 n 项的和，那么 George Andrews 猜想 $m_n \sim n \ln n / \ln \ln n$，且 $M_n \sim n^2 (\ln n)/\ln(\ln n)^2$，并提出了下面一个也许更容易些的问题：证明 $\lim n^{-\Delta} m_n = 0$ 对某些 $\Delta < 2$ 成立；证明 $\lim m_n/n = \infty$；证明 $m_n < p_n$ 对每个 n 成立，其中 p_n 是第 n 个素数.

Jeff Lagarias 对 MacMahon 序列作了一些限制，问序列的后继项仅不包含序列前面两或三相邻项的和时，导出的序列：

1,2,4,5,8,10,12,14,15,16,19,20,21,24,25,27,28,32,33,34,37,38,40,42,43,44,46,47,48,51,53,54,56,57,58,59,61,……

的密率为3/5吗？

[1]G. E. Andrews, MacMahon's prime numbers of measurement, *Amer. Math. Monthly*, 82(1975),922-923.

[2]R. L. Graham, Problem #1910, *Amer. Math. Monthly*, 73(1966), 775; solution, 75(1968), 80-81.

[3]Jeff Lagarias, Problem 17, W. Coast Number Theory Conf., Asilomar, 1975.

[4]P. A. MacMahon, The prime numbers of measurement on a scale, *Proc. Cambridge Philos. Soc.*, 21(1923),651-654.

[5]Štefan Porubský, On MacMahon's segmented numbers and related sequences, *Nieuw Arch. Wisk.*, (3) 25(1977), 403-408; *MR* 58#5575.

[6]N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973; sequences 363,416, 1044.

E25. Hofstadter 的三个序列

Doug Hofstadter 定义了三个有趣的序列

(a) $a_1 = a_2 = 1, a_n = a_{n-a_{n-1}} + a_{n-a_{n-2}} (n \geq 3)$，该序列的性质如何呢？序列给出：

1,1,2,3,3,4,5,5,6,6,6,8,8,8,10,9,10,11,11,12,

12,12,12,16,14,14,16,16,16,16,20,17,17,…

有无穷多个如7,13,15,18,…这样的数不在序列中吗?

(b) $b_1 = 1$,$b_2 = 2$,且对 $n \geqslant 3$,b_n 是比 b_{n-1} 大的最小整数,且能表成此序列两个或更多的相邻项的和,因此有:

1,2,3,5,6,8,10,11,14,16,17,18,19,21,22,24,25,

29,30,32,33,34,35,37,40,41,43,45,46,47,….

此问题是 MacMahon 问题(E24)的孪生问题.现在的问题是,此序列将怎样增长?

(c) $c_1 = 2$,$c_2 = 3$ 且当 $c_1,\cdots,c_n$ 被定义时,形成所有可能的表达式 $c_ic_j - 1(1 \leqslant i < j \leqslant n)$,并把他们作为添加项而得到下面的序列:

2,3,5,9,14,17,26,27,33,41,44,50,51,53,69,77,80,81,84,87,98,99,101,105,122,125,129,…

其结果将包含几乎全部的整数吗?

[1]P. Erdös and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographie de L' Enseignement Mathématique No. 28,Genève, 1980,pp. 83-84.

E26. 由贪心算法得到的 B_2—序列

Dikson 的一个古老问题仍未获解决.给定 k 个整数的集合 $a_1 < a_2 < \cdots < a_k$,对于 $n \geqslant k$,定义 a_{n+1} 为比 a_n 大的最小整数,且它不具有形 $a_i + a_j, i, j \leqslant n$.除了起始的初值外,这些便是由贪心算法得到的 B_2—序列(见 C8,E7,E22).

差 $a_{n+1} - a_n$ 构成的序列最终成周期性变化吗?

在周期性出现以前,也许要花很长时间.例如,对于 $k = 2$,我们取 $a_1 = 1$,$a_2 = 6$,序列为

1,6,8,10,13,15,17,22,24,29,31,33,36,38,40,45,47,52,54,56,59,61,63,68,…

要想认识到这模式，可从集合{1，4，9，16，25}开始.

[1]L. E. Dickson, The converse of Waring's problem, *Bull. Amer. Math. Soc.*, 40(1934), 711-714.

E27. 不含单调算术级数的序列

Erdös 和 Graham 研究了序列 $\{a_i\}$，并认为如果存在下标 $i_1 < i_2 < \cdots < i_k$ 使得子序列 $a_{i_j}(1 \leqslant j \leqslant k)$ 是递增或递减的 AP，则序列 $\{a_i\}$ 有长度为 k 的单调 AP. 长度为 k 的单调 AP 也说是单调的 k 项 AP. 如果 $M(n)$ 是$[1,n]$上满足没有单调的3项 AP 的排列的个数，则 Davis 等人证明了

$$M(n) \geqslant 2^{n-1}, M(2n-1) \leqslant (n!)^2, M(2n+1) \leqslant (n+1)(n!)^2$$

他们问是否 $M(n)^{1/n}$ 有界？

Davis 等人还证明了所有正整数的任何排列必包含一递增的3项 AP，但是，存在没有单调的5项 AP 的排列. 仍不清楚是否有单调的4项 AP.

如果正整数被排成双无穷序列，那么单调3项 AP 仍然必定出现. 但是避免4项 AP 出现是可能的.

如果所有的整数参与排列，那么 Odda 证明了，在单无穷情形下，没有7项 AP 出现，但是其他情形如何，很少为人所知.

[1]J. A. Davis, R. C. Entringer, R. L. Graham and G. J. Simmons, On permutations containing no long arithmetic progressions, *Acta Arith.*, 34(1977), 81-90; *MR* 58#10705.

[2] Tom Odda, Solution to Problem E2440, *Amer. Math. Monthly*, 82(1975), 74.

E28. 一类特殊序列的 Jacobi 符号

柯召对于正整数 x，首先研究了整数序列 $E_n = \frac{x^n - 1}{x - 1}(n \geqslant$

1) 的性质，证明了：在 $x \equiv 0 \pmod 4$ 时，对任意奇数 $m \geqslant 3, n \geqslant 1$，$(m,n)=1$，都有 Jacobi 符号（见 F5）$(E_n/E_m)=1$. 由此导出了 Catalan 方程 $y^2-1=x^n (n \geqslant 3)$（见 D8）仅有正整数解 $x=2, y=3, n=3$. 后来，Terjanian，孙琦和曹珍富又研究了整数序列 $Q_n = \dfrac{x^n-y^n}{x-y}$ 的性质，其中 x, y 是给定的整数，$(x,y)=1$，例如有以下的结果：

1）如果 $xy \equiv 0$ 或 $-1 \pmod 4$，则对任意奇数 $m \geqslant 3, n \geqslant 3$，$(m,n)=1$ 有 $(Q_n/Q_m)=1$；

2）如果 $xy \equiv 1 \pmod 4$，则对任意正奇数 m, n 有 $(Q_n/Q_m)=(n/m)$.

Rotkiewicz 将上述结果还推广到 Lehmer 数 P_n 上，这里

$$P_n=\begin{cases}(\alpha^n-\beta^n)/(\alpha-\beta), \text{当 } 2 \nmid n, \\ (\alpha^n-\beta^n)/(\alpha^2-\beta^2), \text{当 } 2 \mid n,\end{cases}$$

而 α, β 是方程 $z^2-\sqrt{L}z+M=0$ 的两个根，L, M 是整数且满足 $L>0, L-4M>0, (L,M)=1$. 但是，对于 Lucas 数

$$U_n=\varepsilon^n+\eta^n, n \geqslant 0,$$

这里 ε, η 是方程 $z^2-\sqrt{R}z+S=0$ 的两个根，$(R,S)=1$. 要研究类似的问题却十分困难. 曹珍富令

$$U_n=(\varepsilon^n+\eta^n)/(\varepsilon+\eta) (\text{当 } 2 \nmid n),$$

从而问，当 $2 \nmid m$ 时，Jacobi 符号 (U_n/U_m) 的值如何确定？如何估计 $\sum (U_n/U_m)=$？这里 $\sum$ 包含对固定的 m, n 通过 m 缩系. 最近，曹珍富给出了前一问题的回答，但对后一问题仍没有结果.

[1] 曹珍富（Z. Cao），丢番图方程引论，第八章，哈尔滨工业大学出版社，1989，*MR* 92e：11018

[2] 曹珍富（Z. Cao），一类不定方程对 Lucas 序列的应用，数学杂志，11 (1991)，3：267－274，*MR* 93j：11019.

[3] 曹珍富（Z. Cao），关于丢番图方程 $x^p-y^p=Dz^2$，东北数学，2(1986)，2：

219—227; *MR* 88b:11013.

[4]曹珍富(Z. Cao), On the Diophantine equation $x^4 - py^2 = z^p$, *C. R. Math. Rep. Acad. Sci. Canada*, 17(1995), 2:61 — 66; 18(1996), 5:233 — 234.

[5]柯召(C. Ko), 关于方程 $x^2 = y^n + 1, xy \neq 0$, 四川大学学报(自然科学版), 1962, 1:1—6.

[6]A. Rotkiewicz, Applications of Jacobi's symbol to Lehmer's numbers, *Acta Arith.*, 42(1983), 163-187.

[7]孙琦(Q. Sun), 曹珍富(Z. Cao), 关于丢番图方程 $x^p - y^p = z^2$, 数学年刊, *A*, 7(1986), 5:514 — 518; *MR* 88*c*:11022.

[8]G. Terjanian, Sur l'équation $x^{2p} + y^{2p} = z^{2p}$, *C. R. Acad. Sci. Paris*, 285(1977), 973-975.

F 一些其它问题

本章介绍不在前面出现的数论中的一些其它问题，其中有一些问题是近几年才提出的. 头几个问题是关于格点的(其 Euclid 坐标为整数)且他们中的大部分是二维的，但也有一些问题是在更高维数上阐述的. 一些有趣的书是：

[1]J. W. S. Cassels, *Introduction to the Geometry of Numbers*, Springer-Verlag, N. Y. 1972

[2]L. Fejes Tóth, *Lagerungen in der Ebene, auf der Kugel und in Raum*, Springer-Verlag, Berlin, 1953.

[3]J. Hammer, *Unsolved Problems Concerning Lattice Points*, Pitman, 1977

[4]O. H. Keller, *Geometrie der Zahlen*, Enzyclopedia der Math. Wissenschaften, Vol. 12, B. G. Teubner, Leipzig, 1954.

[5]C. G. Lekkerkerker, *Geometry of Numbers*, Bibliotheca Mathematia, Vol. 8, Walters-Noordhoff, Groningen; North-Holland, Amsterdam, 1969.

[6]C. A. Rogers, *Packing and Covering*, Cambridge Univ. Press, 1964

F1. Gauss 格点问题与除数问题

一个非常困难的问题是 Gauss 问题：圆心在原点，半径为 r 的圆内有多少个格点？如果答案是 $\pi r^2 + h(r)$ 个，那么 Hardy 和 Landau 证明了，$h(r)$ 不是 $o(r^{1/2}(\ln r)^{1/4})$，并且猜想 $h(r) = O(r^{1/2+\epsilon})$. 已知的最好结果是属于陈景润的，他证明了 $h(r) = O(r^{24/37+\epsilon})$. 三维时，对球和正则四面体可以提出同样的问题. 例如对球问题，易知

$$\sum_{u^2+v^2+w^2\leqslant x} 1 = \frac{4}{3}\pi x^{3/2} + h_1(x),$$

陈景润证明了 $h_1(x) = O(x^{2/3+\epsilon})$. 尹文霖对除数问题也获得了类似结果. 对三维除数问题,设 $d_3(n)$ 表 n 成三个因子乘积的表法个数,则有

$$\sum_{n\leqslant x} d_3(x) = xp_3(\ln x) + h_2(x),$$

这里 $p_3(\ln x)$ 为 $\ln x$ 的一个二次多项式. 最好的结果是属于尹文霖和李中夫的,他们证明了 $h_2(x) = O(x^{127/282})$.

[1]陈景润(J. Chen),圆内整点问题,数学学报,2(1963),299－313;中国科学,12(1963),633－649; *MR* 27#4799.

[2]尹文霖(W. Yin), $\zeta(1/2 + it)$ 的阶,四川大学学报(自然科学版),1963, 2:63－72.

[3]尹文霖(W. Yin),李中夫,三维除数问题误差项估计的改进,科学通报,16(1980),767.

F2. 不同距离的格点

在格点 (x,y), $1 \leqslant x,y \leqslant n$ 中,使 $\binom{k}{2}$ 个格点相互距离都不同的最大 k 是什么?很容易看出 $k \leqslant n$. $n \leqslant 7$ 时能得到 k 的界. 但是,对任意大的 n 却不能. Erdös 和 Guy 证明了

$$n^{2/3-\epsilon} < k < cn/(\ln n)^{1/4}$$

且猜想 $k < cn^{2/3}(\ln n)^{1/6}$. 人们可以求"浸润"组态,它含有确定不同距离且在不重复某一距离时就无法加进新格点的那些格点的最小个数. Erdös 注意到,这至少需要 $n^{2/3-\epsilon}$ 个格点. 在一维时,他已不能改进 $O(n^{1/3})$,且猜测 $O(n^{1/2+\epsilon})$ 是可能达到的最好的结果.

[1]P. Eedös and R. K. Guy, Distinct distances between lattice points, *Elem. Math.* 25 (1970), 121-123.

F3. 没有4点共圆的格点

Erdős 和 Purdy 问，从 n^2 个格点 (x,y)，$1\leqslant x,y\leqslant n$ 中，能挑出多少个点使得没有4点共圆. 很容易证明能挑出 $n^{2/3-\epsilon}$ 个，但是挑出更多的也是可能的.

选 t 个点使他们确定的 $\binom{t}{2}$ 条直线包含全部 n^2 个格点，那么满足此条件的最小 t 是多少？$t=o(n)$ 吗？不难证明 $t>cn^{2/3}$.

F4. 无三点共线问题

能选出 $2n$ 个格点 $(x,y)(1\leqslant x,y\leqslant n)$ 使得没有三点共线吗？对 $n\leqslant 26$时，这已经实现. Guy 和 Kelly 提出四个猜想：

(1)不存在不具有完全的正方形对称性的矩形对称性的组态.

(2)仅有的具有正方形对称性的组态是 $n=2,4,10$的情形(见下页图13. $n=10$的组态首先由 Acland—Hood 找到).

(3)对于充分大的 n，问题的答案为否定，即该问题只有有限个解.

(4)对大 n，我们至多可选 $(c+\epsilon)n$ 个格点，它们没有三点共线，其中 $3c^3=2\pi^2$，即 $c\approx 1.85\cdots$.

另一方面，Erdős 证明了，如果 n 是素数，则选出 n 个点且没有三点共线是可能的. Hall 等人证明了，对于大 n，能找到$(3/2-\epsilon)n$ 个这样的点.

无三点共线问题是 Heibronn 的30岁问题的离散模拟. 放 $n(\geqslant 3)$ 个点于单位面积(或者单位正方形，或者单位面积的三角形)的盘中，使由其三点形成的最小三角形面积为极大. 如果我们用 $\Delta(n)$ 来表示此极大面积，则 Heilbronn 的原猜想为：$\Delta(n)<c/n^2$. Erdős 证明了，$\Delta(n)>1/(2n^2)$. 因此，如果猜想为真，则它是可能达到的最好结果. K. F. Roth 证明了 $\Delta(n)\ll 1/n(\ln\ln n)^{1/2}$, Schmidt 改进到 $\Delta(n)\ll 1/n(\ln n)^{1/2}$. 接着 Roth 又改进到 $\Delta(n)\ll 1/n^{\mu-\epsilon}$，其中 μ 值开始为 $\mu=2-2/\sqrt{5}>1.1055$，后来又

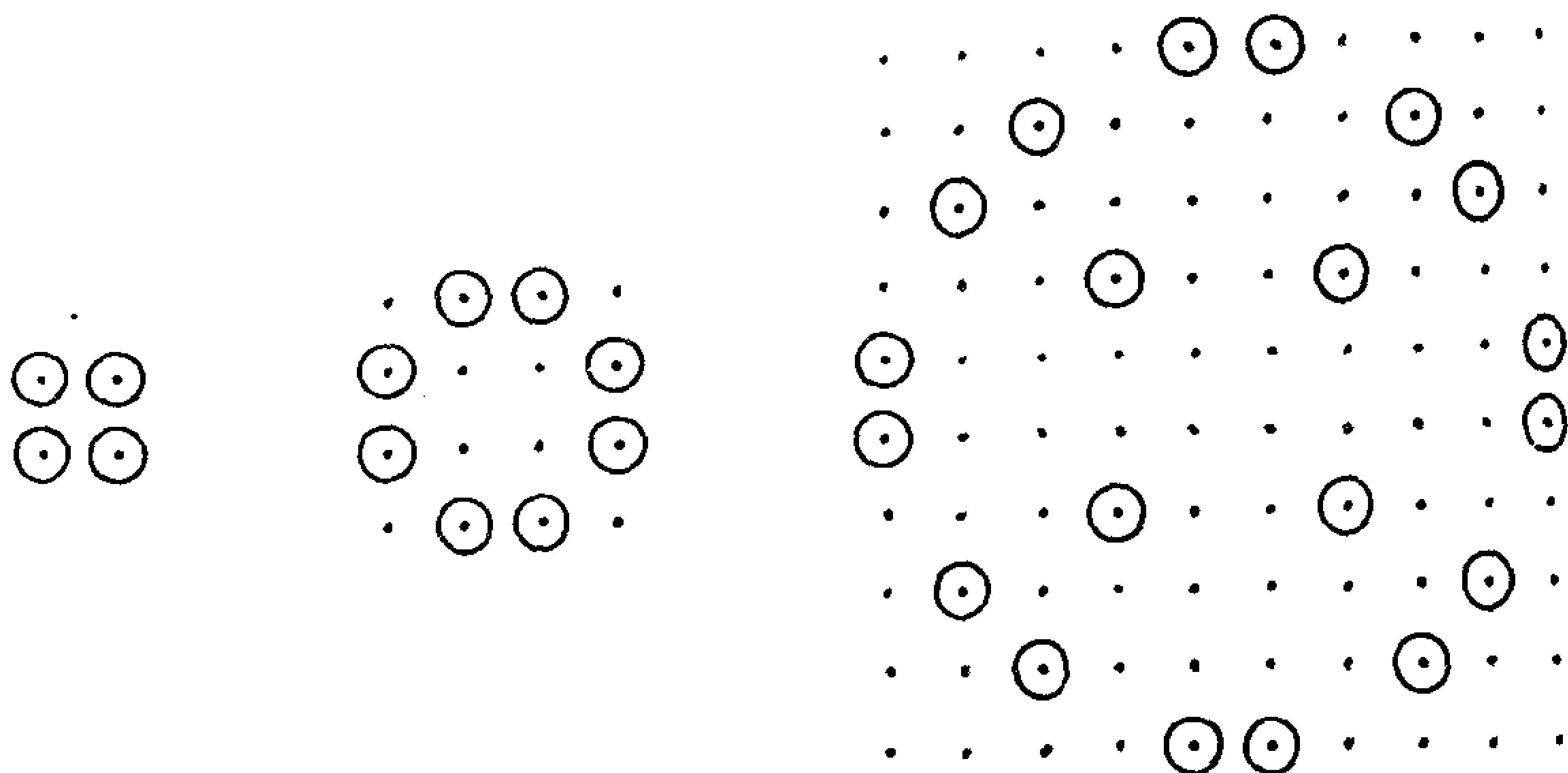


图13. $2n$ 个格点中无三点共线，$n=2,4,10$

得到 $\mu=(17-\sqrt{65})/8>1.1172$.

后来，Komlós，Pintz 和 Szemerédi 把下界改进到 $(\ln n)/n^2$，由此否定 Heilbronn 的猜想，他们还改进了上界.

[1]Acland-Hood, *Bull. Malayan Math. Soc.*, 0(1952-53), E 11-12.

[2]Michael A. Adena, Derek A. Holton and Patrick A. Kelly, Some thoughts on the no-three-in-line problem, Proc. 2nd Austral. Conf. Combin. Math., *Springer Lecture Notes*, 403(1974), 6-17; *MR*; 50# 1890.

[3]David Brent Anderson, Update on the no-three-in-line problem, *J. Combin. Theory Ser. A*, 27 (1979), 365-366.

[4]W. W. Rouse Ball and H. S. M. Coxeter, *Mathematical Recreations and Essays*, 12th ed Univ. of Toronto Press, 1974, p. 189.

[5]D. Craggs and R. Hughes-Jones, On the no-three-in-line problem, *J. Combin. Theory Ser. A*, 20(1976), 363-364; *MR* 53# 10590.

[6]H. E. Dudeney, *Amusements in Mathematics*, Nelson, London, 1917, 94, 222

[7]Martin Gardner, Mathematical Games; Challenging chess tasks for puzzle

butts and answers to the recreational puzzles, *Sci. Amer.*, 226 # 5(May 1972), 112-117, esp pp. 113-114.

[8] Martin Gardner, Mathematical Games: Combinatorial problems, some old, some new and all newly attacked by computer, *Sci. Amer.*, 235 # 4(Oct 1976), 131-137, esp. pp. 133-134 also 236 # 3(Mar 1977), 139-140.

[9] Michael Goldberg, Maximizing the smallest triangle made by N points in a square, *Math. Mag.*, 45(1972), 135-144.

[10] Richard K. Guy, *Bull. Malayan Math. Soc.*, 0(1952-53), E 22.

[11] Richard K. Guy, Unsolved combinatorial problems, in D. J. A. Welsh, *Combinatorial Mathematics and Its Applications*, Academic Press, London, 1971, p. 124.

[12] Richard K. Guy and Patrick A. Kelly, The no-three-in-line problem, *Canad. Math. Bull.*, 11(1968), 527-531.

[13] R. R. Hall, T. H. Jackson, A. Sudbery and K. Wild, Some advances in the no-three-in-line problem, *J. Combin Theory Ser. A*, 18(1975), 336-341.

[14] P. A. Kelly, The use of the computer in game theory, M. Sc. thesis, Univ. of Calgary, 1967

[15] Torleiv Klove, On the no-three-in-line problem II, *J. Combin. Theory Ser. A*, 24(1978), 126-127; *MR* 57 # 2962; *Zbl.* 393. 05004.

[16] Torleiv Klove, On the no-three-in-line problem III, *J. Combin. Theory Ser. A*, 26(1979), 82-83; *Zbl.* 393. 05005.

[17] Carl Pomerance, Collinear subsets of lattice point sequences-an analog of Szemerédi's theorem, *J. Combin. Theory Ser. A*, 28(1980), 140-149.

[18] K. F. Roth, On a problem of Heibronn, *J. Landon Math. Soc.* 25 (1951), 198-204, esp. Appendix p. 204; Ⅱ, Ⅲ, *Proc. London Math. Soc.*, 25(1972), 193-212, 543—549.

[19] K. F. Roth, Developments in Heibronn's triangle problem, *Advances in Math.*, 22(1976), 364-385; *MR* 55 # 2771.

[20] Wolfgang M. Schmidt, On a problem of Heilbronn. *J. London Math.*

Soc. 4(1971/72) 545-550.

F5. 二次剩余、Schur 猜想

素数 p 的二次剩余是指非零数 $r(<p)$，使得同余式 $r\equiv x^2 \pmod{p}$ 有解. 模 p 的二次剩余共有 $(p-1)/2$ 个，且如果 p 具有 $4k+1$ 的形式，则它是对称分布的. 如果 $p=4k-1$，那么用 Dirichlet 的类数公式很容易证明：位于区间 $[1,2k-1]$ 中的二次剩余比 $[2k,4k-2]$ 中要多.

对于头几个 d 值，很容易证明哪些素数取 d 为二次剩余.

$d=-1$	$p=4k+1$		
$d=-2$	$p=8k+1,3$	$d=2$	$p=8k\pm 1$
$d=-3$	$p=6k+1$	$d=3$	$p=12k\pm 1$
$d=-5$	$p=20k+1,3,7,9$	$d=5$	$p=10k\pm 1$
$d=-6$	$p=24k+1,5,7,11$	$d=6$	$p=24k\pm 1,5.$

但是，在这些小 d 的情形中，偶尔有剩余随 d 符号的不同，恰在周期的前1/2或后1/4中. Legendre 符号 $\left(\frac{a}{p}\right)$ 常被用来表示与素数 p 互素的数 a 的二次特征，它的值随 a 是或不是 p 的二次剩余而取 ±1. 例如，$\left(\frac{-1}{p}\right)$ 随 $p=4k\pm 1$ 而取 ±1.

Legendre 符号的一个有用的推广是 Jacobi 符号 $\left(\frac{a}{b}\right)$，这里 $(a,b)=1$，b 为奇数，它由 Legendre 符号的积

$$\prod\left(\frac{a}{p_i}\right)$$

来定义，其中 $b=\prod p_i$ 是 b 的素数分解(其中允许某些 p_i 相同). 这些符号重要的特性包括：如果 $a\equiv c \pmod{p}$，则 $\left(\frac{a}{p}\right)=\left(\frac{c}{p}\right)$ 及 Gauss 著名的二次互反定律：对奇素数 p,q，$\left(\frac{p}{q}\right)=$

$\left(\frac{q}{p}\right)$，除非 p,q 都$\equiv -1 \pmod 4$，而此时，$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$. 这些特性可用来迅速判断一个相当大数的二次特征. 如 224 对 325 的 Jacobi 符号为

$$\left(\frac{224}{325}\right)=\left(\frac{224}{5\times 5\times 13}\right)=\left(\frac{224}{5}\right)\left(\frac{224}{5}\right)\left(\frac{224}{13}\right)$$

$$=\left(\frac{224}{13}\right)=\left(\frac{3}{13}\right)=\left(\frac{13}{3}\right)=\left(\frac{1}{3}\right)=1.$$

这个过程说明，224是5的二次剩余，224还是13的二次剩余，所以224是325的二次剩余. 事实上，$224\equiv 43^2 \pmod{325}$.

如果 R（相应为 N）是奇素数 p 的连续二次剩余（相应为非二次剩余）的最大个数，那么，A. Brauer 证明了，对 $p\equiv 3 \pmod 4$，$R=N<\sqrt{p}$；另一方面，如果 $p=13$，则 $N=4>\sqrt{13}$，因为5，6，7，8都是13的非二次剩余. Schur 猜想：如 p 充分大，则 $N<\sqrt{p}$. Hudson 证明 Schur 猜想是正确的；此外，他认为 $p=13$是仅有的例外.

[1]A. Brauer, Über die Verteilung der potenzreste, *Math. Z.*, 35(1932), 39—50; *Zbl.* 3, 339

[2]H. Davenport, *The Higher Arithmetic*, Hutchinson's Univ. Library, 1952, 74-78.

[3]Richard H. Hudson, On sequences of quadratic nonresidues, *J. Number Theory*, 3(1971), 178-181; *MR*43#150.

[4]Richard H. Hudson, On a conjecture of Issai Schur, *J. reine angew. Math.*, 289(1977), 215-220; *MR* 58#16481.

F6. 二次剩余的模式

对任意正奇数 $n>1$为模，必定出现什么样的二次剩余？很容易看出，连续二次剩余对是一定存在的. 因为2，5和10中至少有一个是二次剩余，因此(1，2)，(4，5)或(9，10)便是这样的对. 同样地，

(1,3),(2,4)或(4,6)中至少有一个是差为2的二次剩余对;(1,4)是差为3的对;(1,5),(4,8),(6,10)或(12,16)中至少有一个是差为4的对;如此等等.

假定 r, $r+a$, $r+b$ 中的每一个都是模 p 的二次剩余. Emma Lehmer 问:对于所有充分大的 p,哪组 (a,b),使得 $r, r+a, r+b$ 都为模 p 的二次剩余?用 $\Omega(a,b)$ 表对所有 $p>p(a,b)$, $r\leqslant\Omega(a,b)$ 使得 $r, r+a, r+b$ 为模 p 二次剩余的最小 r. 如果不存在有限数,则记 $\Omega(a,b)=\infty$,例如,Emma Lehmer 证明了 $\Omega(1,2)=\infty$,且更一般地,如果 $(a,b)\equiv(1,2)\pmod 3$, $(a,b)\equiv(1,3),(2,3)$ 或 $(2,4)\pmod 5$, $(a,b)\equiv(1,5),(2,3)$ 或 $(4,6)\pmod 7$,则 $\Omega(a,b)=\infty$. 那在余下的情形里,$\Omega(a,b)$ 为有限吗?Emma Lehmer 猜想,如果 a,b 为平方数,则它是有限的. 当然,如果 a,b 均比平方数小,则 $\Omega(a,b)=1$. 作为例子,让我们看看为什么 $\Omega(5,23)=16$. 如果(1,6,24)和(4,9,27)都不全为二次剩余,则6和3不是,而2必

表9: $\Omega(a,b)$ 的值 ($a<b\leqslant 25$)

$b=$ / a	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	a
1	45	∞	24	38	∞	84	26	∞	∞	∞	∞	77	35	∞	∞	∞	∞	15	35	∞	21	69	1
2	∞	25	20	∞	∞	∞	∞	70	30	∞	∞	54	∞	∞	∞	∞	25	98	∞	∞	∞	∞	2
3	174	39	∞	∞	1	∞	55	∞	∞	36	105	1	∞	∞	18	36	95	∞	∞	∞	1	51	3
4		∞	∞	∞	∞	91	36	∞	∞	∞	∞	126	60	∞	38	168	∞	90	∞	∞	66	77	4
5			49	∞	∞	121	∞	25	4	∞	28	∞	∞	64	110	∞	100	4	∞	16	64	∞	5
6				57	∞	33	30	∞	24	∞	42	60	36	38	∞	62	78	60	78	∞	45	∞	6
7					∞	∞	75	∞	74	∞	∞	27	8	∞	∞	∞	∞	70	42	∞	∞	45	7
8						66	∞	∞	∞	∞	30	1	∞	∞	77	∞	48	∞	∞	42	1	∞	8
9							∞	54	∞	42	66	57	66	∞	36	27	16	72	∞	21	∞	119	9
10								∞	60	85	∞	55	∞	∞	32	102	∞	77	26	∞	28	39	10
11									28	∞	119	49	∞	39	∞	∞	∞	64	∞	∞	25	∞	11
12										∞	∞	∞	65	98	∞	∞	36	4	∞	∞	∞	90	12
13											∞	42	∞	∞	∞	36	∞	∞	∞	∞	36	∞	13
14												35	∞	∞	42	∞	52	56	∞	64	81	∞	14
15													66	27	69	∞	49	25	99	110	1	105	15
16														∞	∞	102	∞	169	95	∞	∞	56	16
17															∞	∞	76	64	∞	∞	∞	∞	17
18																81	∞	∞	∞	40	185	144	18
19																	∞	33	∞	∞	36	96	19
20																		74	∞	40	25	∞	20
21																			93	∞	70	100	21
22																				∞	∞	98	22
23																					∞	∞	23
24																						63	24

定是二次剩余. 如果(2,7,25)和(13,18,36)都不全为二次剩余，则7和13必须是二次非剩余. 在这些前提下，$(r, r+5, r+23)$ 对$1 \leqslant r \leqslant 15$不全为二次剩余，但是当$r=16$时，(16,21,39)为二次剩余.

表9(见前页)列出被认为是最小的 $\Omega(a,b)$ 的值. 这也为除开已经讨论过情形外，$\Omega(a,b)$ 均是有限的猜想提供了好的证据. 就 a,b 来说能得到它们的上界吗？

对于多个变元的情形又如何呢？

[1]D. H. Lehmer and Emma Lehmer, On runs of residues, *Proc. Amer. Math. Soc.*, 13(1962), 102-106; *MR* 25#2035.

[2]D. H. Lehmer. Emma Lehmer and W. H. Mills, Pairs of consecutive power residues, *Canad. J. Math.* 15(1963), 172-177; *MR* 26#3660.

F7. Pell 方程的三次模拟

Hugh Williams 注意到，如果素数 $p \equiv 3 \pmod 4$，那么方程 $x^2 - py^2 = 2$ 仅当 $w^2 \equiv 2 \pmod p$ 成立时有整数解，即 $\left(\frac{2}{p}\right) = 1$时有整数解. 并问方程 $x^3 + py^3 + p^2z^3 - 3pxyz = 3$ ($p \not\equiv \pm 1 \pmod 9$)是否仅当 $w^3 \equiv 3 \pmod p$ 成立时有解？Barrucand 和 Cohn 证明了这对 $p \equiv 2$或$5 \pmod 9$时为真. 那么 $p \equiv 4$或$7 \pmod 9$的情形又怎样呢？这是 Barrucand 那个一般猜想的特殊情形. 如果它为真，那么它在寻找三次域 $Q(\sqrt[3]{p})$ 的基本单位时很有用.

[1]P.-A. Barrucand and Harvey Cohn, A rational genus, class number divisibility and unit theory for pure cubic fields, *J. Number Theory*, 2 (1970), 7-21.

[2]H. C. Williams, Improving the speed of calculating the regulator of certain pure cubic fields, *Math. Comp.*, 35(1980), 1423-1434.

F8. Ebert 问题

Gary Ebert 问:模 p^n 二次剩余 r_i 的最大集是什么?其中 $p^n \equiv 1 \pmod 4$ 使得对全部 (i,j),$r_i - r_j$ 为模 p^n 的二次剩余.

F9. 原根

素数 p 的原根 g 是这样定义的:它使得 $g, g^2, \cdots, g^{p-1} = 1$ 的剩余类都是不同的.例如5是23的原根,因为:

$$5, 5^2 \equiv 2, 5^3 \equiv 10, 4, -3, 8, -6, -7, 11, 9, -1,$$
$$-5, -2, -10, -4, 3, -8, 6, 7, -11, -9, 1$$

都属于不同的剩余类(mod23).

Erdös 问:如果 p 充分大,那么总存在素数 $q < p$ 使得 q 是 p 的原根吗?

Basil Gordon 问是否每一奇素数 p 都有一原根 $g > (p-1)/2$ 也为素数?

给定一素数 $p > 3$,Brizolis 问是否总存在 p 的原根 g 及 $x(0 < x < p)$ 使得 $x \equiv g^x \pmod p$.如果是,那么 g 又能被选择使得 $0 < g < p$ 和 $(g, p-1) = 1$吗?

Vegh 问,对所有素数 $p > 61$,是否每一整数都能表成 p 的两原根之差?在 $p > 2^{60}$ 时,这个问题的回答是肯定的,而且更一般的,孙琦与李曙光证明了:如果 $p > 2^{60}$,$a, b, c \in Z_{p^l}$,$p \nmid abc$,则至少有 $(p-2)p^{l-2}$ 对模 p^l 的原根 α, β 使得 $a\alpha + b\beta \equiv c \pmod{p^l}$.

如果 p 和 $q = 4p^2 + 1$ 都为素数,Gloria Gagola 问,是否对全部 $p > 3$,3是 q 的原根;$p = 193$是否是仅有的奇素数,其2不是 q 的原根?$p = 653$是不是仅有的素数,它使得5既不是 q 的二次剩余也不是 q 的原根;存在(也许是 p 的函数,诸如 $2p-1$,这里 p 很大)总是 q 的原根的数吗?

[1]孙琦(Q. Sun),李曙光,On primitive roots mod p^l,*Chinese Sci. Bull.*, 34(1989),9:714—715.

F10. 2的幂的剩余

Graham 问 2^n 对模 n 的剩余如何?在 $n>1$ 时,$2^n\equiv 1\pmod n$ 不存在解,$2^n\equiv 2\pmod n$ 在 n 是以2为底的伪素数(见 A12)时成立,特别地,只要 n 为素数也成立. Lehmer 已证明 $2^n\equiv 3\pmod n$ 的最小解是 $n=4700063497=19\times 47\times 5263229$. 当然 n 必须是合数;且它不能被2,3,7,17,,31,41,43,73,…中的任何一个除尽. 这些素数是什么?

F11. 模 p 剩余系中的一些问题

对每一个 $x(0<x<p)$,其中 p 是奇素数,现由 $x\bar{x}\equiv 1\pmod p$ 且 $0<\bar{x}<p$ 来定义 $\bar{x}$. 设 N_p 表 x 和 $\bar{x}$ 具有相反奇偶性的个数,例如,对 $p=13$, $(x,\bar{x})=(1,1)$,$\underline{(2,7)}$,$(3,9)$,$(4,10)$,$\underline{(5,8)}$,$\underline{(6,11)}$,$(12,12)$,因此 $N_{13}=6$. D. H. Lehmer 要求找到 N_p 或至少关于它做一点非平凡的事情. 随 $p\equiv\pm 1\pmod 4$ 而有 $N_p\equiv 2$ 或 $0\pmod 4$. $N_3=N_7=0$;$N_5=2$;$N_{11}=N_{19}=N_{31}=4$;$N_{13}=6$;$N_{17}=10$;$N_{23}=12$ 和 $N_{29}=18$. 曹珍富令 $\overline{N}_p$ 表示 x 和 $\bar{x}$ 具有相同奇偶性的个数,则 $\lim\limits_{p\to\infty}\frac{N_p}{\overline{N}_p}=1$ 吗?是否无穷多次出现1?大于1?或小于1?

F12. 覆盖系

如果每一整数 y 对至少一个 i 满足 $y\equiv a_i\pmod{n_i}$,则称同余系 $a_i\pmod{n_i}$ $(1\leqslant i\leqslant k)$ 为覆盖系. 例如0(mod 2),0(mod 3),1(mod 4),5(mod 6),7(mod 12)是覆盖系. 如果 $c=n_1<n_2<\cdots<n_k$, Erdös 为有任意大 c 的覆盖系的存在性证明或反例提供500美元奖金. Davenport 和 Erdös,及 Fried 找到了 $c=3$时的覆盖系;Swift 找到了 $c=6$;Selfridge 找到了 $c=8$;Churchhouse 找到了 $c=10$;Selfridge 找到了 $c=14$,Krukenberg 找到 $c=18$,且 Choi 找

到 $c=20$.

Erdős 为所有模 n_i 均是不同的奇的且比1大的覆盖系不存在的证明提供25美元的奖金，而 Selfridge 为举出这样一个系的明白无误的例子提供500美元奖金. 更一般地，“奇”能用“不被前 r 个素数除尽”来代替. Jim Jordan 愿意为上面提到的那些问题对于高斯整数(A16)时的解提供相当可观的奖金.

Erdős 注意到，用210的真因子能得到一覆盖系，其所有的模 n_i 是不同的，无平方因子的且比1大：

a_i	0	0	0	1	0	1	1	2	2	23	4	5	59	104
n_i	2	3	5	6	7	10	14	15	21	30	35	42	70	105

Krukenberg 用2和大于3的无平方因子数也得到此列. Selfridge 问用 $c\geqslant 3$ 来替代2时是否能得到这样的系. 他注意到 n_i 不可能都是至多有两个素因子的无平方因子数，但是，上面的例子表明，不需要比三个更多.

很容易但不是平凡地证明：对于不同模 n_i 的覆盖系有 $\sum_{i=1}^{k} 1/n_i > 1$. 如果 $n_1=3$ 或4，则和能无限地接近1. 张明志证明，不同模中存在子集 $\{n_{i_1},\cdots,n_{i_t}\}$ 使得 $\sum_{j=1}^{t} 1/n_{i_j}\equiv 0 \pmod 1$. Selfridge 和 Erdős 猜想，$\sum 1/n_i > 1+c_{n_1}$，其中 c_{n_1} 随 n_1 趋向∞.

Erdős 也阐述了下面的猜想：考虑所有奇数的算术级数，如果这些奇数没有一项是 2^k+p 形式，那么所有这些级数都能从覆盖同余得到吗？有无穷多个不具有 2^k+p 形式的整数不在这样的级数中吗？

$$127,149,251,331,337,373,509,599,701,$$
$$757,809,877,905,907,959,977,997,\cdots$$

中哪个数不在这样的级数中？

[1]S. L. G. Choi, Covering the set of integers by congruence classes of dis-

tinct moduli, *Math. Comp.*, 25(1971), 885-895; *MR* 45#6744.

[2]R. F. Churchhouse, Covering sets and systems of congruences, in *Computers in Mathematical Research*, North-Holland, 1968, 20-36; *MR* 39#1399.

[3]Fred Cohen and J. L. Selfridge, Not every number is the sum or difference of two prime powets, *Math. Comp.*, 29 (1975), 79-81.

[4]P. Erdős, Some problems in number theory, in *Computers in Number Theory*, Academic Press, 1971, 405-414; esp. pp. 408-409.

[5]J. Haight, Covering systems of congruences, a negative result, *Mathematika*, 26(1979), 53-61; *MR* 81e:10003.

[6]J. H. Jordan, Covering classes of residues, *Canad. J. Math.*, 19 (1967), 14-519; *MR* 35#1538.

[7]J. H. Jordan, A covering class of residues with odd moduli, *Acta Arith.*, 13(1967-68), 335-338; *MR* 36#3709.

[8]C. E. Krukenberg, PhD thesis, Univ. of Illinois, 1971, 38-77.

[9]A. Schinzel, Reducibility of polynomials and covering systems of congruences, *Acta Arith.*, 13(1967), 91-101; *MR* 36#2596.

[10]张明志(M. Zhang),覆盖剩余系的一个注记,四川大学学报(自然科学版),26(1989),特辑:185-188.

F13. 恰覆盖系

如果一个同余系既是覆盖又是不相交的(即每一个整数恰被一个同余式覆盖),那么它被称为恰覆盖系(也称不相交覆盖系).为恰覆盖系 $a_i \pmod{n_i}$ $(1 \leqslant i \leqslant k)$ 的必要的但不是充分的条件是 $\sum_{i=1}^{k} 1/n_i = 1$ 且 $(n_1, n_2, \cdots, n_k) > 1$. 张明志进一步证明了必要条件 $\sum_{j=1}^{k} a_j/n_j = (k-1)/2$ (见 F12所附文献). Znám 猜想,如果 $[n_1, n_2, \cdots, n_k] = \prod p_j^{\alpha_j}$,那么 $k \geqslant 1 + \sum \alpha_j (p_j - 1)$. 1974年,Korec 证明了这一猜想(参看柯召,孙琦的书). 后来,Znam 证明了,如果 p 是 n_k 的最小素因子,那么 $n_k = n_{k-1} = \cdots = n_{k-p+1}$. 从而推广了 Davenport, Mirsky, Newman 和 Rado 等人的结果. 他猜想,

如果仅存在成对的等模，那么模便都具有 $2^\alpha 3^\beta$ 的形式. 但是后来，他和 Schönheim 又给出了反例：

mod	5	10	15	30	20	40	60	120
	0,1	2,7	3,8	13,28	4,9	14,34	19,39	59,19

Stein 证明了如果仅存在一对等模，其余的均不同，那么 $n_i = 2^i (1 \leqslant i \leqslant k-1), n_k = 2^{k-1}$. 类似地，Znám 证明了如果存在三个相等的模，其余的均不同，那么 $n_i = 2^i (1 \leqslant i \leqslant k-3), n_{k-2} = n_{k-1} = n_k = 3 \times 2^{k-3}$. 主要的问题是给出恰覆盖同余的特征.

[1]N. Burshtein and J. Schönheim, On exactly covering systems of congruences having moduli occurring at most twice, *Czechoslovak Math. J.*, 24 (99)(1974), 369-372; *MR* 50#4521.

[2]A. S. Fraenkel, A characterization of exactly covering congruences, *Discrete Math.*, 4(1973), 359-366.

[3]柯召(C. Ko)，孙琦，数论讲义(上)，第二章 §10，高等教育出版社，1986.

[4]Bretislav Novák and Štefan Znám, Disjoint covering systems, *Amer. Math. Monthly*, 81(1974), 42-45.

[5]Š. Znám, On Mycielski's problem on systems of arithmetical progressions, *Colloq. Math.*, 15(1966), 201-204; *MR* 34#134.

[6]Š. Znám, On exactly covering systems of arithmetic sequences, *Math. Ann.*, 180(1969), 227-232; *MR* 39#4087.

[7]Š. Znám, A simple characterization of disjoint covering systems, *Discrete Math.* 12(1975), 89-91.

F14. Graham 的一个问题

Graham 为解决下列问题提供25美元的奖金，即：$0 < a_1 < a_2 < \cdots < a_n$ 蕴含 $\max_{i,j} a_i/(a_i, a_j) \geqslant n$ 吗？

如果上述不等式不成立，则 Marica 和 Schönheim 证明了至少有一个 a_i 有 >1 的平方因子；Winterle 证明了，a_1 不是素数；Sze-

meredi 证明了 n 不是素数；Weinstein 证明了如果某个 a_i 是素数 p，则对一些 j，k 有 $p=\frac{a_j+a_k}{2}$；Vélez 证明了 $n-1$ 不是素数，且如果素数 p 除尽某些 a_i，那么 $p \leqslant n$；Boyle 改进此结果到 $p \leqslant (n-1)/2$ 且对许多情形改进到 $p \leqslant (n-1)/3$；Simpson 证明了没有 a_i 为素数. 最近，Alexandru 对充分大的 n 证明了上述不等式成立.

[1] Z. Alexandru, On a conjecture of Graham, *J. Number Theory*, 27 (1987), 33-40.

[2] R. D. Boyle, On a problem of R. L. Graham, *Acta Arith.*, 34 (1978), 163-177.

[3] E. Z. Chein, On a conjecture of Graham concerning a sequence of integers, *Canad. Math. Bull.*, 21 (1978), 285-287; *MR* 80d: 10024; *Zbl.* 392. 10002.

[4] P. Erdös, Problems and results in combinatorial number theory, in *A Survey of Combinatorial Theory*, North-Holland, 1973, 117-138.

[5] R. L. Graham, Advanced problem 5749*; *Amer. Math. Monthly*, 77 (1970) 775.

[6] J. Marica and J. Schönheim, Differences of sets and a problem of Graham, *Canad. Math. Bull.*, 12 (1969), 635-637.

[7] R. J. Simpson, On a conjecture of R. L. Graham, *Acta Arith.*, 40 (1982), 209-211.

[8] William Ysals Vélez, Some remarks on a number theoretic problem of Graham, *Acta Arith.*, 32 (1977), 233-238.

[9] Gerald Weinstein, On a conjecture of Graham concerning greatest common divisors, *Proc. Amer. Math. Soc.*, 63 (1977), 33-38; *Zbl.* 369. 10003.

[10] Riko Winterle, A problem of R. L. Graham in combinatorial number theory, *Congressus Numerantium* I, Proc. Conf. Combin. Baton Rouge, Utilitas Math. Pub. 1970. 357-361; *MR* 42#3051.

F15. 小素数幂的乘积

Erdős 定义 $A(n,k)$ 为 $\prod p^{a}$，其中积取遍小于 k 的素数 p，且 $p^{a}\| n$，他问：

$$\max_{n}\min_{1\leqslant i\leqslant k} A(n+i,k)=o(k)?$$

他说很易证明它是 $O(k)$.

$$\max_{n}\min_{1\leqslant i\leqslant k} A(n+i,k)>k^{c}$$

对于每一个 c 和充分大的 k 成立吗？

$$\sum_{i=1}^{k}\frac{1}{A(n+i,k)}>c\ln k?$$

F16. 与 ζ-函数有关的级数

Alf van der Poorten 要求证明

$$\zeta(4)\left[=\sum_{n=1}^{\infty}\frac{1}{n^{4}}=\frac{\pi^{4}}{90}\right]=\frac{36}{17}\sum_{n=1}^{\infty}\frac{1}{n^{4}\binom{2n}{n}}.$$

已知

$$\sum_{n=1}^{\infty}\frac{1}{\binom{2n}{n}}=\frac{2\pi\sqrt{3}+9}{27},\ \sum_{n=1}^{\infty}\frac{1}{n\binom{2n}{n}}=\frac{\pi\sqrt{3}}{9},$$

$$\zeta(2)\left[=\sum_{n=1}^{\infty}\frac{1}{n^{2}}=\frac{\pi^{2}}{6}\right]=3\sum_{n=1}^{\infty}\frac{1}{n^{2}\binom{2n}{n}},$$

$$2(\sin^{-1}x)^{2}=\sum_{n=1}^{\infty}\frac{(2x)^{2n}}{n^{2}\binom{2n}{n}}$$

和

$$\zeta(3)\left[=\sum_{n=1}^{\infty}\frac{1}{n^3}\right]=\frac{5}{2}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^3\binom{2n}{n}}.$$

但是，人们怎样证明 $\zeta(4)$ 的结果？

[1]Louis Comtet, *Advanced Combinatorics*, Dreidel, Dordrecht, 1974, p. 89.

[2]Alfred van der Poorten, A proof that Euler missed…Apery's proof of the irrationality of $\zeta(3)$. An informal report, *Math. Intelligencer*, 1 (1979), 195－203.

[3]Alfred J. van der Poorten, Some wonderful formulas…an introduction to poly-logarithms, *Proc. Number Theory Conf. Queen's Univ.*, Kingston, 1979. 269-286; *MR* 80i:10054.

F17. n 个数成对的和与积的集合

如果 $a_1, a_2, \cdots, a_n$ 是 n 个数（任意类），那么他们成对的和与积的集合多大呢？

$$|\{a_i+a_j\}\cup\{a_ia_j\}|>n^{2-\epsilon}?$$

Erdős 和 Szemerédi 已证明 $|\{a_i+a_j\}\cup\{a_ia_j\}|>n^{1+\epsilon}$.

[1]P. Erdős, Some recent problems and results in graph theory, combinatorics and number theory, *Congressus Numerantiun XVII*, Proc. 7th S. E. Conf. Combin. Graph Theory, Comput. Boca Raton, 1976, 3-14 (esp. p. 11)

F18. 最大积的素数分拆

如果 n 充分大且记 $n=a+b+c, 0<a<b<c$，那么在每一种可能的方式中，所有积 abc 都不同吗？

J. Riddell 和 H. Taylor 问，在 n 分为不同素数和的分解中，具有最大积的分解其个数一定最多吗？但是 Selfridge 给出了否定的回答，例如：

$$319=2+3+5+7+11+13+17+23+29+31+37+41+47+53$$
$$=3+5+11+13+17+19+23+29+31+37+41+43+47,$$

分解成的个数较少的却给出了可能是最大的积. 这是最小的反例吗?两个集合的基数差能是任意大吗?

F19. 连分数

x 能被表成连分数

$$x=a_0+\cfrac{b_1}{a_1+\cfrac{b_2}{a_2+\cdots}}$$

出于排字方便的考虑,通常记为

$$x=a_0+\frac{b_1}{a_1+}\,\frac{b_2}{a_2+}\,\frac{b_3}{a_3+}\cdots$$

当分子 b_i 全为1时,连分数被称为简单的. 他可以是有限的或无限的. 但如果 x 是有理数,则它是有限的. 在这种情形下,存在两种可能的形式,其中之一是它的最后部分商 a_k 等于1:

$$\frac{7}{16}=\frac{1}{2+}\,\frac{1}{3+}\,\frac{1}{2}=\frac{1}{2+}\,\frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{1}$$

并不是每一个 n 都能表成两正整数 a 与 b 的和,它使 b/a 的连分数所有部分商等于1或2. 对于11,17,19我们有:

$$\frac{4}{7}=\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{1},\ \frac{5}{12}=\frac{1}{2+}\,\frac{1}{2+}\,\frac{1}{2}\text{ 和 }\frac{7}{12}=\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{2}$$

但是23就不能如此表达. Leo Moser 猜想:有一个常数 c 使得,每个 n 表达的部分商的和 $\sum a_i<c\ln n$.

F20. Rotkiewicz 问题

Rotkiewicz 提出下面的三个问题.

(a)设 $p>3,\neq 9$,是一个给定的奇数,问是否存在奇数 q 使得 Jacobi 符号(见 F5) $\left(\frac{q}{p}\right)=(-1)^{\lambda}$ 和 $\frac{p}{q}=c_1+\frac{1}{c_2+}\cdots\frac{1}{c_\lambda}$, 这里

$c_\lambda > 1$.

(b)设 $M_p = \{n \mid (\frac{n}{p}) = (-1)^\lambda, 0 < n < p$ 且 $\frac{p}{n} = c_1 + \frac{1}{c_2 +} \cdots \frac{1}{c_\lambda}, c_\lambda > 1\}$，$\overline{M}_p = \{n \mid (\frac{n}{p}) = (-1)^{\lambda+1}, 0 < n < p$ 且 $\frac{p}{n} = c_1 + \frac{1}{c_2 +} \cdots \frac{1}{c_\lambda}, c_\lambda > 1\}$，令 $N(p) = |M_p|$，$\overline{N}(p) = |\overline{M}_p|$. 试找到函数 $N(p)$，$\overline{N}(p)$ 的下界和上界.

(c) $\lim\limits_{p \to \infty} \frac{N(p)}{\overline{N}(p)} = 1$成立吗？

曹珍富首先给出了问题(a)的肯定回答，同时，他还证明了，设 $p \equiv 1 \pmod 4$，$p > 1$，则 $N(p) = \overline{N}(p)$，而在 $p \equiv 3 \pmod 4$时，他的结果支持他提出如下猜想：

(d) $\overline{N}(p) \geqslant N(p) \geqslant 2$.

(e) $\lim\limits_{p \to \infty} \frac{N(p)}{\overline{N}(p)} = 1$不成立.

[1]曹珍富(Z. Cao)，关于 Rotkiewicz 的一个问题，数学研究与评论，2 (1987)，318－320.

[2]A. Rotkiewicz, Application of Jacobi's symbol to Lehmer's numbers, *Acta Arith.*, ALII(1983)，163－187.

F21. 部分商为 *a* 或 *b* 问题

Bohuslav Divis 要求证明：在每一个实二次域中，存在一个无理数，其简单连分数所有的部分商等于1或2. 他对用任意对不同的自然数替代1和2问了同样的问题.

F22. 无界部分商的代数数

存在一个代数数(次数大于2)其连分数有无界的部分商吗？每一个次数大于2的实代数数都有无界的部分商吗？Ulam 特别地问到 $\zeta = \frac{1}{(\zeta + y)}$，其中 $y = \frac{1}{(1 + y)}$ 如何？

Littlewood 注意到，如果 θ 存在具有有界部分商 a_n 的连分数，那么 $\lim\inf n\ |\sin n\theta| \leqslant A(\theta)$，其中 $A(\theta)$ 不是0(尽管对几乎所有的 θ 它是零). 他问

$$\lim\inf n\ |\sin n\theta \sin n\varphi| = 0$$

对所有实的 θ 和 φ 都成立吗？已知对几乎所有的 θ 和 φ 成立. 另一方面，

$$\lim\inf n^{1+\epsilon}\ |\sin n\theta \sin n\varphi| = \infty$$

对几乎所有的 θ 和 φ 成立. Cassels 和 Swinnerton-Dyer 解决了一个孪生问题且顺便证明了 $\theta = 2^{1/3}, \varphi = 4^{1/3}$ 给不出反例. Davenport 认为计算机也许有助于证明 $|(x\theta - y)(x\varphi - z)| < \varepsilon$ 对于每一个 θ, φ 有解，例如当 $\varepsilon = \frac{1}{10}$ 或 $\frac{1}{50}$ 时.

[1]J. W. S. Cassels and H. P. F. Swinnerton-Dyer, On the product of three homogeneous linear forms and indefinite ternary quadratic forms, *Philos. Trans. Roy. Soc. London Ser. A* 248(1955), 73-96; *MR* 17-14.

[2]Harold Davenport, Note on irregularities of distribution, *Mathematika*, 3 (1956), 131-135; *MR* 19,19,

[3]John E. Littlewood, *Some Problems in Real and Complex Analysis*, Heath, Lexington Mass., 1968, 19-20, Problems 5, 6

F23. 用2的幂逼近某些数

Littlewood 问：如何用 2^m 去逼近 3^n，使 $3^n - 2^m$ 与 2^m 的比尽可能小？他给出一个例子

$$\frac{3^{12}}{2^{19}} = 1 + \frac{7183}{524288} \approx 1 + \frac{1}{73}.$$

Croft 对 $n! - 2^m$ 问了相应的问题. 2的幂对 $n!$ 的头几个最好的近似是：

5!　　20!　　22!　　24!　　61!　　63!

2^7	2^{61}	2^{70}	2^{79}	2^{278}	2^{290}
-1.33	$+0.126$	-0.10	$+0.047$	$+0.023$	-0.0017

其中，第三行是指数误差比的百分数，例如设 $5! = 2^x$，则 -1.33 是 $(x-7)/7$ 的百分数. Erdös 注意到 $n! = 2^a \pm 2^b$ 仅当 $n = 1,2,3,4$ 和5成立.

F24. 两个不同数字组成的平方数

Sin Hitotumatu 要求证明下述问题或举出它的反例：除开 10^{2n}，4×10^{2n} 和 9×10^{2n} 外，仅存在有限多个平方数恰由两不同十进制数字组成，如：

$1444 = 38^2$，$7744 = 88^2$，$11881 = 109^2$，$29929 = 173^2$，$44944 = 212^2$，$55225 = 235^2$ 和 $9696996 = 3114^2$.

F25. 数的住留度

在序列679，378，168，48，32，6中，每一项都是前项十进制数字的积. Neil Sloane 定义一个数的住留度为：一个数在下降到一位数以前的步数（例中为5步）. 我们有

10，25，39，77，679，6788，68889，2677889，26888999，3778888999，277777788888899

的住留度分别为：

$$1,2,3,4,5,6,7,8,9,10,11.$$

住留度大于11的数都大于 10^{50}. Sloane 猜想，存在一个数 c，使得对全部的数其住留度均 $\leqslant c$.

在二进制数中最大的住留度是1. 在三进制中，任何数的数字之积只能是0或2的幂. 人们猜想，比 2^{15} 大的所有2的幂当记为三进制时包含0. 已知此猜想对不超过 2^{500} 的2的幂都为真. 此猜想的真实性将蕴含三进制数的最大住留度是3.

Sloane 的一般猜想是，存在数 $c(b)$ 使得 b 进制数的住留度不

能超过 $c(b)$.

Erdös 设 $f(n)$ 是 n 的非零十进制数字的积，他问，一个数到达1位数能多快？且哪个数下降最慢？他说易于证明 $f(n) < n^{1-c}$，因此至多需要 $c \ln \ln n$ 步.

[1]N. J. A. Sloane, The persistence of a number, *J. Recreatianal Math.*, 6 (1973), 97-98.

F26. 用1表示数

用1和任意个＋和×号来表达 n，设 $f(n)$ 是1的最少个数，由

$64=(1+1+1+1)\times(1+1+1+1)\times(1+1+1+1)$,

$80=(1+1+1+1+1)\times(1+1+1+1)\times(1+1+1+1)$,

知 $f(64) \leqslant 12$, $f(80) \leqslant 13$. 能够证明 $f(3^k)=3k$ 且 $3\log_3 n \leqslant f(n) \leqslant 5\log_3 n$，其中 log 以3为底，那么 $f(n) \sim 3\log_3 n$（对于 $n \to \infty$）？Rawsthorne 对 $n \leqslant 3^{10}(=59049)$ 计算了 $f(n)$. 同时，他令 $S(m)=\{n: f(n)=m\}$，对 $1 \leqslant m \leqslant 37$，他证明了：如果 $b(m)$ 和 $b_1(m)$ 是 $S(m)$ 的最大和次最大的元素，那么 $b_1(m)=[(8/9)b(m)]$. 对更大的 m，$b_1(m)$ 与 $b(m)$ 的关系如何？怎样确定它们？

[1]J. H. Conway and M. J. T. Guy, π in four 4's, *Eureka*, 25(1962), 18-19.

[2]Popken and K. Mahler, On a maximum problem in arithmetic, *Nieuw Arch. voor Wisk.*, (3)1(1953), 1-15.

[3]Daniel A. Rawsthorne, How many 1's are needed? *Fibonacci Quart.*, 27 (1989), 1:14-17.

F27. Farey 级数

阶为 n 的 Farey 级数是指0与1之间的诸既约分数中，分母、分子 $\leqslant n$，且次序按大小排列. 例如，阶为5的 Farey 级数是：

表10　按根大小排列的二次方程系数行列式

a	b	c	根	行列式
0	1	0	0	
2	2	−1	$(\sqrt{3}-1)/2$	1
1	2	−1	$\sqrt{2}-1$	0
0	2	−1	$\frac{1}{2}$	0
0	2	−1	$\frac{1}{2}$	0
1	1	−1	$(\sqrt{5}-1)/2$	0
2	0	−1	$\sqrt{2}/2$	−1
1	2	−2	$\sqrt{3}-1$	−1
2	1	−2	$(\sqrt{17}-1)/4$	1
0	1	−1	1	0
0	1	−1	1	0
2	−1	−2	$(\sqrt{17}+1)/4$	0
2	−2	−1	$(\sqrt{3}+1)/2$	1
1	0	−2	$\sqrt{2}$	−1
1	−1	−1	$(\sqrt{5}+1)/2$	1
0	1	−2	2	0
0	1	−2	2	0
1	−2	−1	$\sqrt{2}+1$	1
1	−2	−2	$\sqrt{3}+1$	0
0	0	1	∞	

$$\frac{1}{5}\ \frac{1}{4}\ \frac{1}{3}\ \frac{2}{5}\ \frac{1}{2}\ \frac{3}{5}\ \frac{2}{3}\ \frac{3}{4}\ \frac{4}{5}\ \frac{1}{1}\ \frac{5}{4}\ \frac{4}{3}\ \frac{3}{2}\ \frac{5}{3}\ \frac{2}{1}\ \frac{5}{2}\ \frac{3}{1}\ \frac{4}{1}\ \frac{5}{1},$$

其两相邻分数分子、分母构成的行列式值是±1. Mahler 把序列的元素看作为一线性方程的正实根，此方程的系数的最大公约数为1且系数本身不超过n，他对二次方程得到下面明显的推广. 按根的

大小列出有正实根的二次方程：$ax^2+bx+c=0, a\geqslant 0, (a,b,c)=1, b^2\geqslant 4ac, \max\{a,|b|,|c|\}\leqslant n$ 的系数 (a,b,c)，则由表10（见前页）知由 a,b,c 三相邻行组成的三阶行列式（见 F28）值为0或± 1.

表10中，对 $n=2$，从0，1，0开始，它对应于0根的情况. 为避免出现平凡的例外，Selfridge 建议重复有理根. 此表以0，0，1结束. 表中最后一列是行列式的值. 该行列式是由该行及与此相邻的上、下行组成.

表10能够证明吗？它能推广到与3次方程相联系的4阶行列式吗？

F28. 值为1的一个行列式

三阶行列式 $\begin{vmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{vmatrix}$ 可定义为 $a_1(a_5a_9-a_6a_8)-a_2(a_4a_9-a_6a_7)+a_3(a_4a_8-a_5a_7)$. Basil Gordon 问：使得

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{vmatrix} = 1 = \begin{vmatrix} a_1^2 & a_2^2 & a_3^2 \\ a_4^2 & a_5^2 & a_6^2 \\ a_7^2 & a_8^2 & a_9^2 \end{vmatrix}$$

成立的全部的数字 $a_1, a_2, \cdots, a_9$ 是什么？（其中没有一个为0或± 1）.

F29. 两个同余式

给定一素数 p，试找到函数 $f(x), g(x)$ 使得同余式 $f(x)\equiv n, g(x)\equiv n \pmod p$ 之一对所有整数 n 可解. 一平凡的例子是 $f(x)=x^2, g(x)=ax^2$，其中 a 是奇素数 p 的二次非剩余. Mordell 给出进一步的例子，$f(x)=2x+dx^4, g(x)=x-1/4dx^2$，其中 d 是与 p 互素的任意整数，且 $1/z$ 被定义为 $\bar{z}$，其中 $z\cdot\bar{z}\equiv 1 \pmod p$.

F30. 一个整除问题

Znám 曾问，是否对每一整数 $n>1$，都存在整数 $x_i>1(i=1,\cdots,n)$ 使得对每一个 i，x_i 是 $x_1\cdots x_{i-1}x_{i+1}\cdots x_n+1$ 的真因子？这个问题已经被孙琦解决. 设 $Z(n)$ 表示 Znám 问题的解 $(x_1,\cdots,x_n)$ $(1<x_1<\cdots<x_n)$ 的个数，他证明了 $Z(n)\geqslant\Omega(n)-\Omega(n-1)(n>1)$，这里 $\Omega(n)$ 是方程

$$(A)\qquad \sum_{j=1}^{n}\frac{1}{x_j}+\frac{1}{x_1\cdots x_n}=1,1<x_1<\cdots<x_n$$

的解的个数(D10). 由于他和曹珍富依次证明了：当 $n\geqslant10$ 时，$\Omega(n+1)\geqslant\Omega(n)+3$；当 $n\geqslant10$ 时 $\Omega(n+1)\geqslant\Omega(n)+5$；当 $n\geqslant11$ 时，$\Omega(n+1)\geqslant\Omega(n)+8$；当 $n\geqslant11$ 时，$\Omega(n+1)\geqslant\Omega(n)+17$ 和当 $n\geqslant11,2\nmid n$ 时，$\Omega(n+1)\geqslant\Omega(n)+23$，且最近曹珍富等证明了当 $n\geqslant11$ 时 $\Omega(n+1)\geqslant\Omega(n)+39$，当 $2\nmid n\geqslant11$ 时 $\Omega(n+1)\geqslant\Omega(n)+57$，故在 $n\geqslant12$ 时 $Z(n)\geqslant39$ 且在 $n\geqslant12$ 时，$2|n$ 时，$Z(n)\geqslant57$. 但是，要得出 $Z(n)$ 的渐近公式仍很不易. 孙琦和曹珍富提出如下猜想：当 $n\geqslant4$ 时，$Z(n+1)>Z(n)$.

类似于 Znám 问题，曹珍富提出了如下问题：对任意给定的正整数 a 是否对每一个整数 $n>1$，都存在整数 $x_i>1(i=1,\cdots,n)$ 使得对每一个 i，x_i 是 $ax_1\cdots x_{i-1}x_{i+1}\cdots x_n+1$ 的真因子？当 $a\equiv7,18,22 \pmod{25}$ 时，这个问题已被解决(参阅 D26).

另一个与方程(A)是孪生的方程是

$$(B)\qquad \sum_{j=1}^{n}\frac{1}{x_j}-\frac{1}{x_1\cdots x_n}=1,1<x_1<\cdots<x_n,$$

设解的个数为 $A(n)$，则已知当 $n\geqslant9$ 时，$A(n+1)\geqslant\Omega(n)+\Omega(n-1)+78$ 且当 $n\geqslant12,2|n$ 时，$A(n+1)\geqslant\Omega(n)+\Omega(n-1)+104$. 可见 $A(n)$ 远远大于 $\Omega(n)$. 曹珍富问：$\lim\limits_{n\to\infty}\dfrac{\Omega(n)}{A(n)}=?$ 他曾提出如下的猜想：当 $n>1$ 时 $A(n+1)>A(n)$.

[1]曹珍富(Z. Cao),丢番图方程引论,哈尔滨工业大学出版社,1989,第417—423页.

[2]曹珍富(Z. Cao),刘锐,张良瑞,On the Equation $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=1$ and Znám's problem, *J. Number Theory*, 27(1987),206—211.

[3]曹珍富(Z. Cao),数论中的一些新的问题和结果,河池师专学报,1(1987),1—8.

[4]孙琦(Q. Sum),关于 Znám 问题,四川大学学报(自然科学版),4(1983),9—11

[5]孙琦(Q. Sun),曹珍富,关于方程 $\sum_{j=1}^{n}\frac{1}{x_j}+\frac{1}{x_1\cdots x_n}=1$,数学研究与评论,1(1987),125—128.

[6]孙琦(Q. Sun),曹珍富,On the Equation $\sum_{j=1}^{s}\frac{1}{x_j}+\frac{1}{x_1\cdots x_s}=n$ and the Number of Solution of Znám's Problem,数学进展,3(1986),329—330.